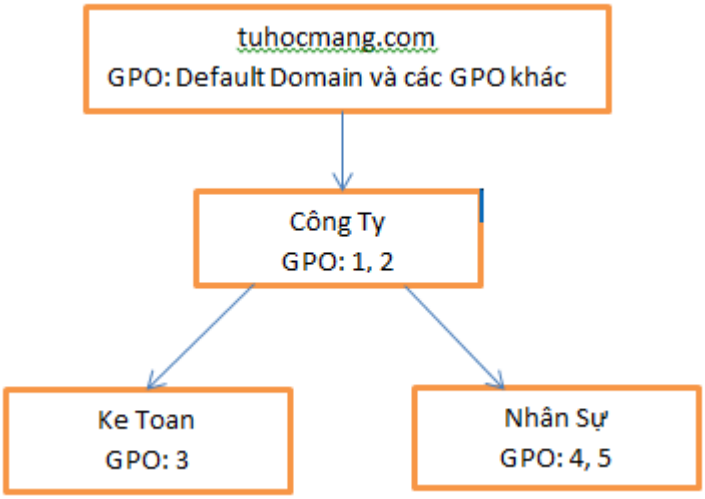
4. Group Policy Object – Phần 1

Chuẩn bị:

+ máy DC: Windows server 2012, (may1, IP: 192.168.1.10/255.255.255.0)

+ máy computer member domain: Windows server 2012, (may2, 192.168.1.2/255.255.255.0)

Tạo cấu trúc OU theo hình cây: OU CongTy chứa 2 OU con là KeToan, NhanSu. Trong OU KeToan chứa: Group KT và user KT1, user KT2. OU NhanSu làm tương tự (Group NS và user NS1, user NS2).



Việc xây dựng OU ngoài mục đích dễ quản lý, dễ dàng ủy nhiệm cho việc quản lý thì chức năng quan trọng của OU là giúp ta triển khai chính sách (policy) ở cấp độ domain. Group Policy bao gồm 2 loại: local policy và domain policy. Local Policy chỉnh ở đâu thì chỉ có nơi đó tác động. Domain Policy thì chỉ cần chỉnh ở 1 nơi mà tác động ở nhiều nơi (toàn Domain hoặc các OU cụ thể).

Để triển khai bộ Domain Policy thì ta phải thông qua một đối tượng (AD object) trung gian là Group Policy Object (GPO). Riêng với Local Policy thì ta chỉnh trực tiếp (gpedit.msc: Local Group Policy Editor). GPO là 1 AD object dùng để chứa những policy được thiết lập nhằm tác động trên hệ thống, 1 GPO có thể chứa 1 hoặc nhiều Policy khác nhau. Cùng 1 Policy có thể chứa trên nhiều GPO khác nhau.

Lưu ý:

+ Trên 1 GPO chỉ nên chỉnh 1 Policy hoặc 1 nhóm Policy có quan hệ với nhau về mặt luận lý (vd: 1 nhóm policy liên quan đến OU KeToan).

+ Đặt tên GPO phải tường minh, mô tả được chức năng của policy (VD: GPO1 – restrict control panel)

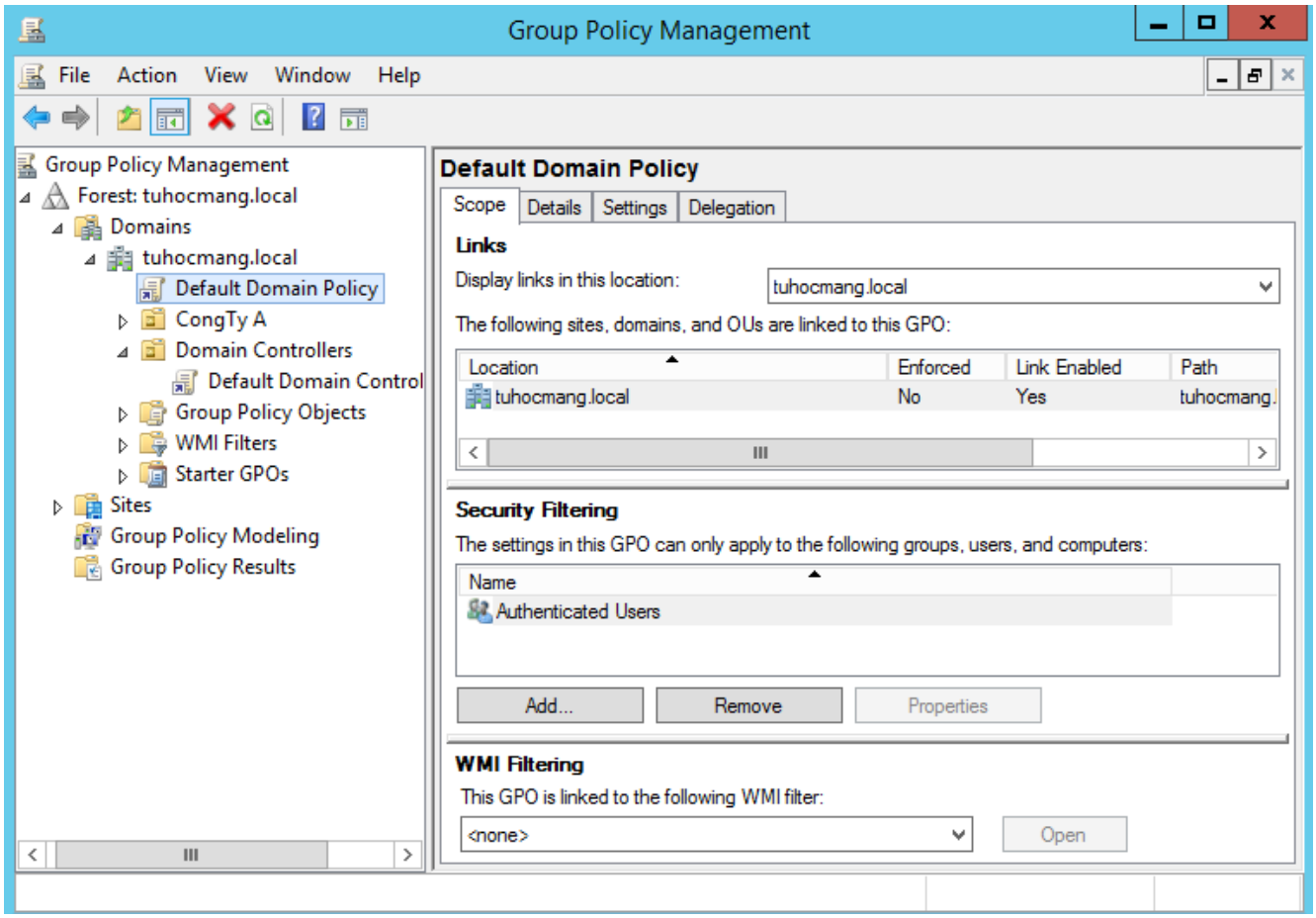
+ GPO chỉ tác động lên 3 đối tượng (object) trong AD (Active Directory): OU, User, Computer account.

(GPO có thể tác động vào nhiều OU, User, computer account và ngược lại). Như vậy Group không bị tác động.

+ GPO có tính kế thừa: GPO mà tác động domain thì tất cả các đối tượng đều bị tác động. GPO tác động lên 1 OU thì các đối tượng bên trong (OU con, user, computer) đều bị tác động . Do đó các chính sách chung của công ty, của phòng ban ta có thể dùng tính kế thừa để triển khai nhanh gọn.

Mở Công cụ quản lý GPO

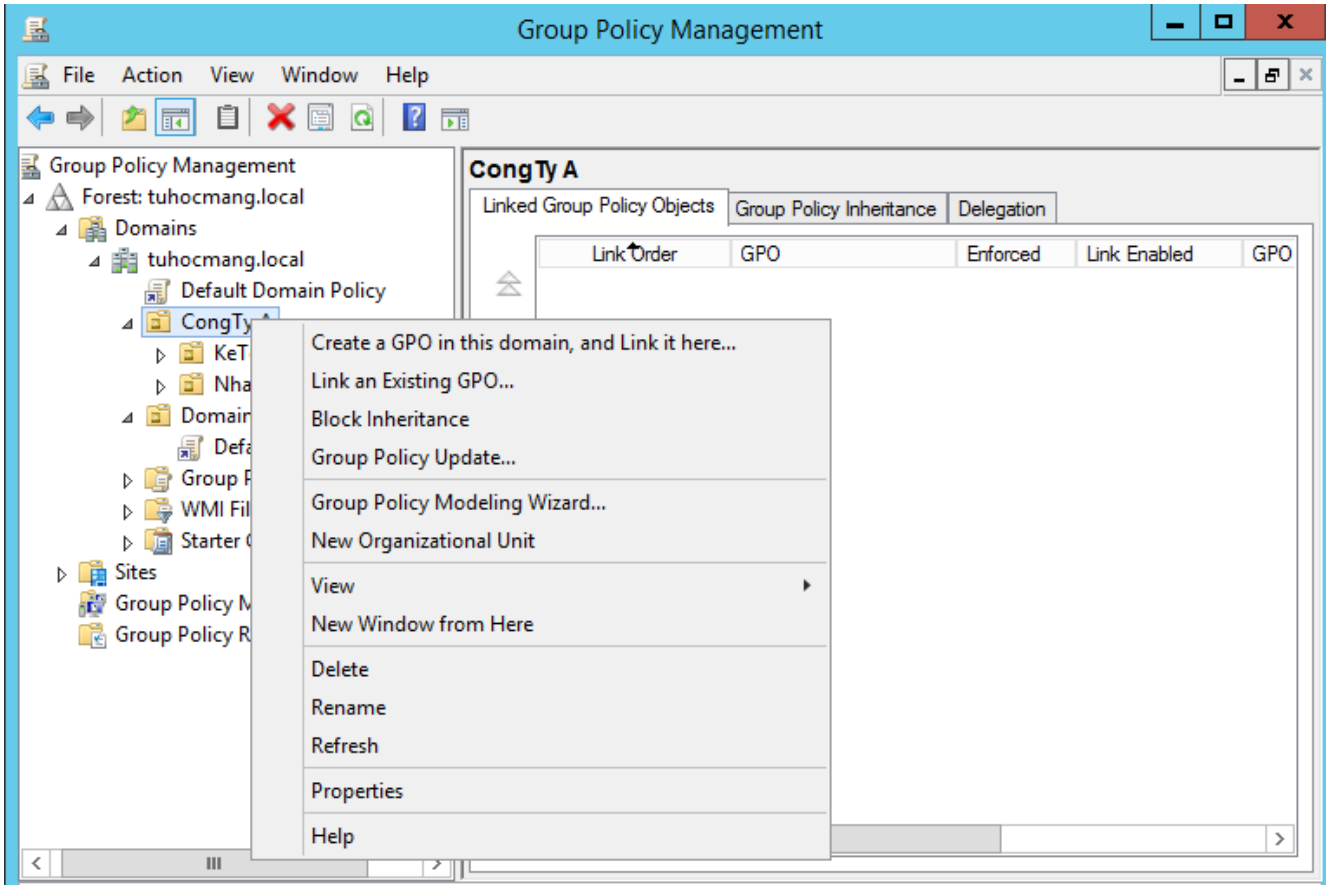
Run -> gpmc.msc: Group Policy Management hoặc vào Tools - > Group Policy Management



gpmc.msc

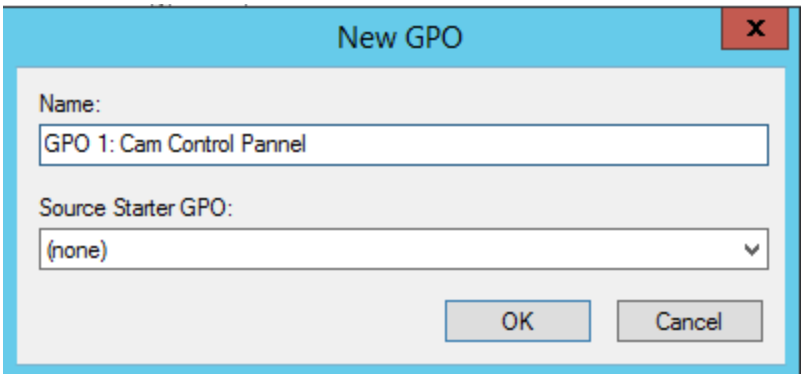
Domain Controller Security Policy: Là GPO tác động đến OU Domain Controller (là OU chứa DC). GPO này chỉ tác động đến DC.

Công ty có nhu cầu : Nhân viên công ty bị cấm vào **Control Panel** => **Tạo GPO ở OU công ty** (lưu ý: GPO tác động tới đâu thì làm việc ở vị trí đó)



Policy

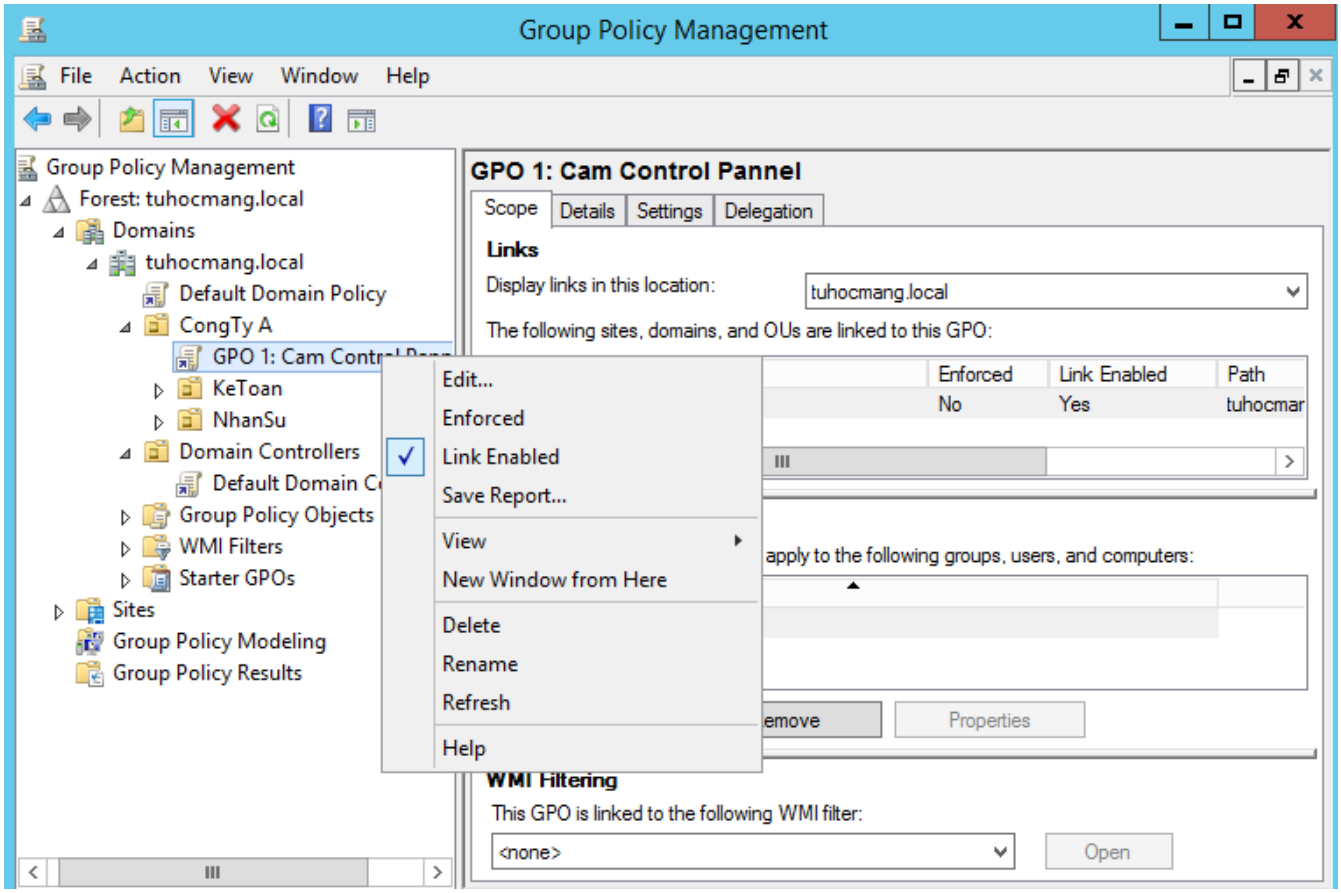
Chọn vào **OU CongTy** -> **Create a GPO in this domain and Link it here …**



Create GPO

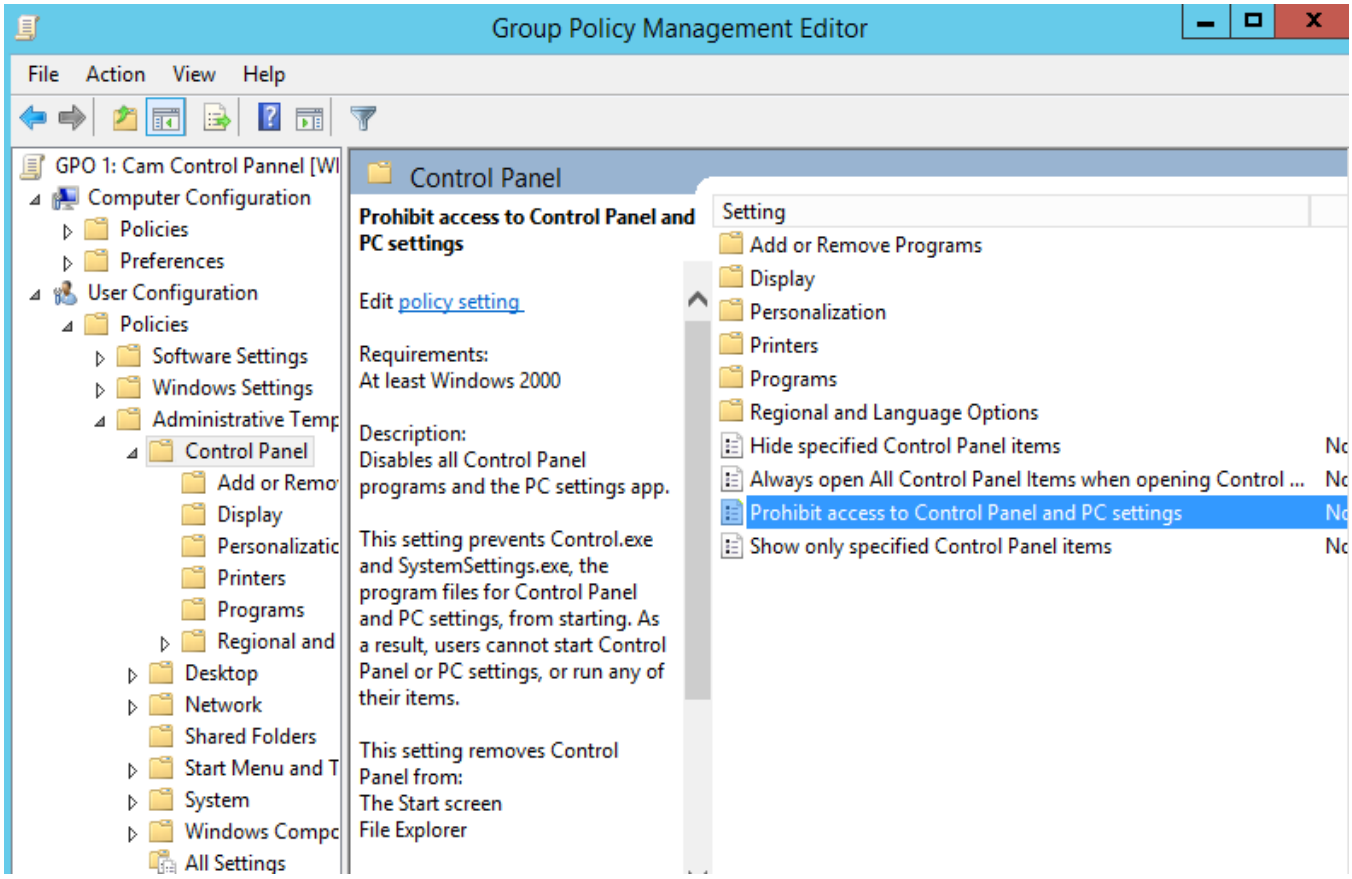
Khai báo tên GPO -> OK

Sau khi tạo GPO xong, **phải chuột GPO** -> **Edit** để tìm Policy cấm control panel



Edit

Enable Policy này lên.



Cấm Control Panel

Tương tự tạo thêm các policy trên OU CongTy:

+ GPO 2: ẩn Recycle Bin

(Administrative Teplates -> Desktop -> Remove Recycle Bin icon…, **Enable** Policy này lên)

Sau khi thực hiện các chính sách của công ty thì các phòng ban cũng có các chính sách riêng.

+ **Phòng Kế Toán**: **Ẩn IE, ẩn My Documents trên màn hình**

GPO 3: An IE, An My Documents

(Administrative Teplates -> Desktop -> Hide IE icon…, Remove My Documents icon… và Enable các Policy này lên).

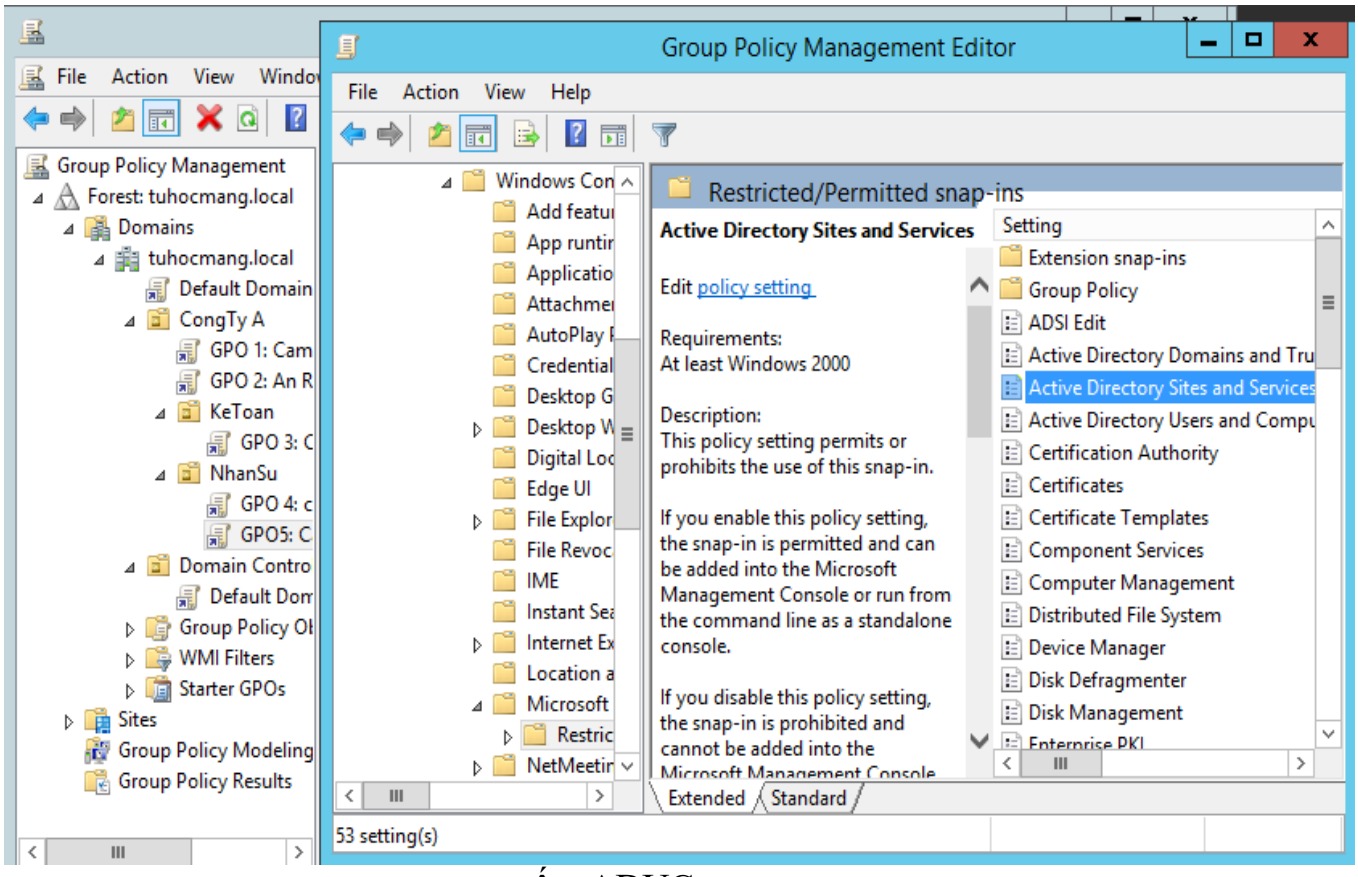
+ **Phòng Nhân Sự**: Cấm sử dụng command line, cấm mở công cụ Active Directory Users and Computers.

GPO 4: Cam cmd

GPO5: Cam mo ADUC (Active Directory Users and Computers)

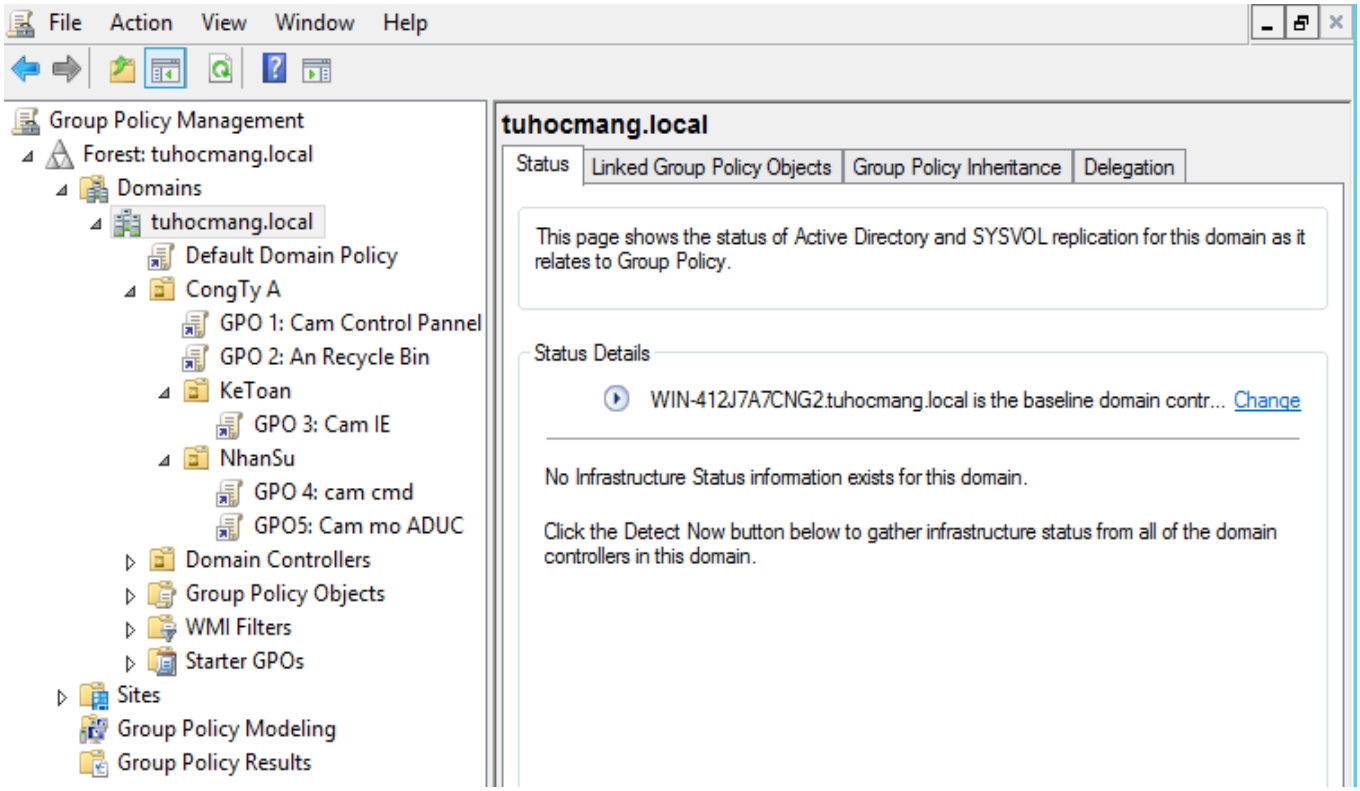
Cách chỉnh GPO5: User configuration ->Policies -> Administrative template -> Windwos Component -> Microsoft Management Console -> Restricted/ Permitted Snap-in -> Active Directories Sites and Services

Ta Enbale Policy này

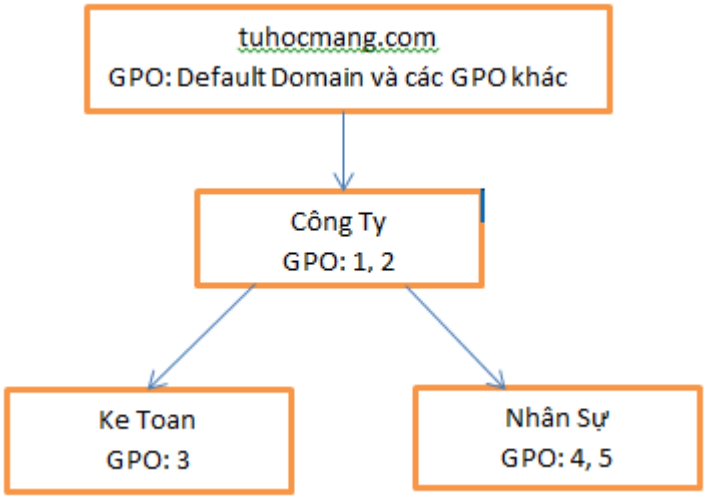


cấm ADUC

Sau đó mở cmd và chạy lệnh **gpupdate /force**



Các GPO áp đặt



Sơ đồ

Ta Test từng user thì thấy rằng:

User KT1, KT2 sẽ chịu ảnh hưởng của GPO: Default Domain Policy, 1, 2, 3.

User NS1, NS2 sẽ chịu ảnh hưởng của GPO: Default Domain Policy, 1, 2, 4, 5

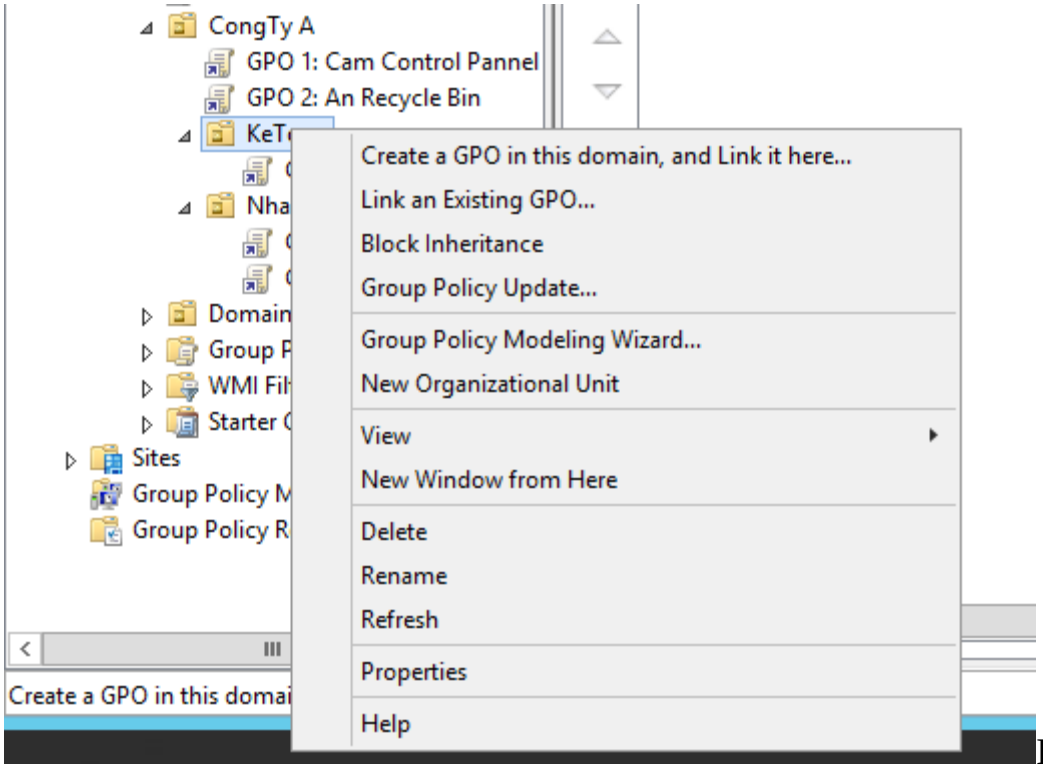
Group KeToan và NhanSu không bị ảnh hưởng.

=> **Chúng ta đã thấy tính kế thừa của GPO.**

Tình huống:

Ta muốn cấm các user trong OU KeToan mở ADUC. Thay vì phải tạo thêm 1 GPO tác động lên OU KeToan thì ta chỉ cần lấy GPO 5 tác động lên OU KeToan. Ta sử dụng tính năng " Link" của GPO.

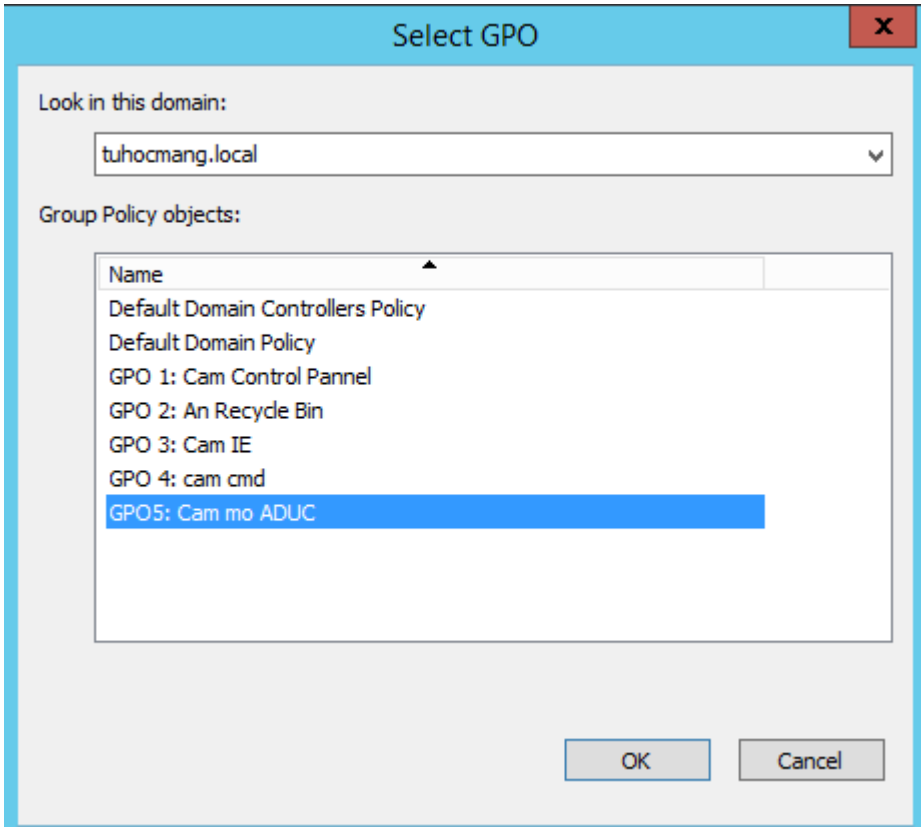
Ta chọn vào OU KetToan -> chọn **Link an existing GPO**



Link GPO

Xuất hiện giao diện SELECT GPO

Ta chọn GPO 5 (hoặc các GPO khác tùy nhu cầu)

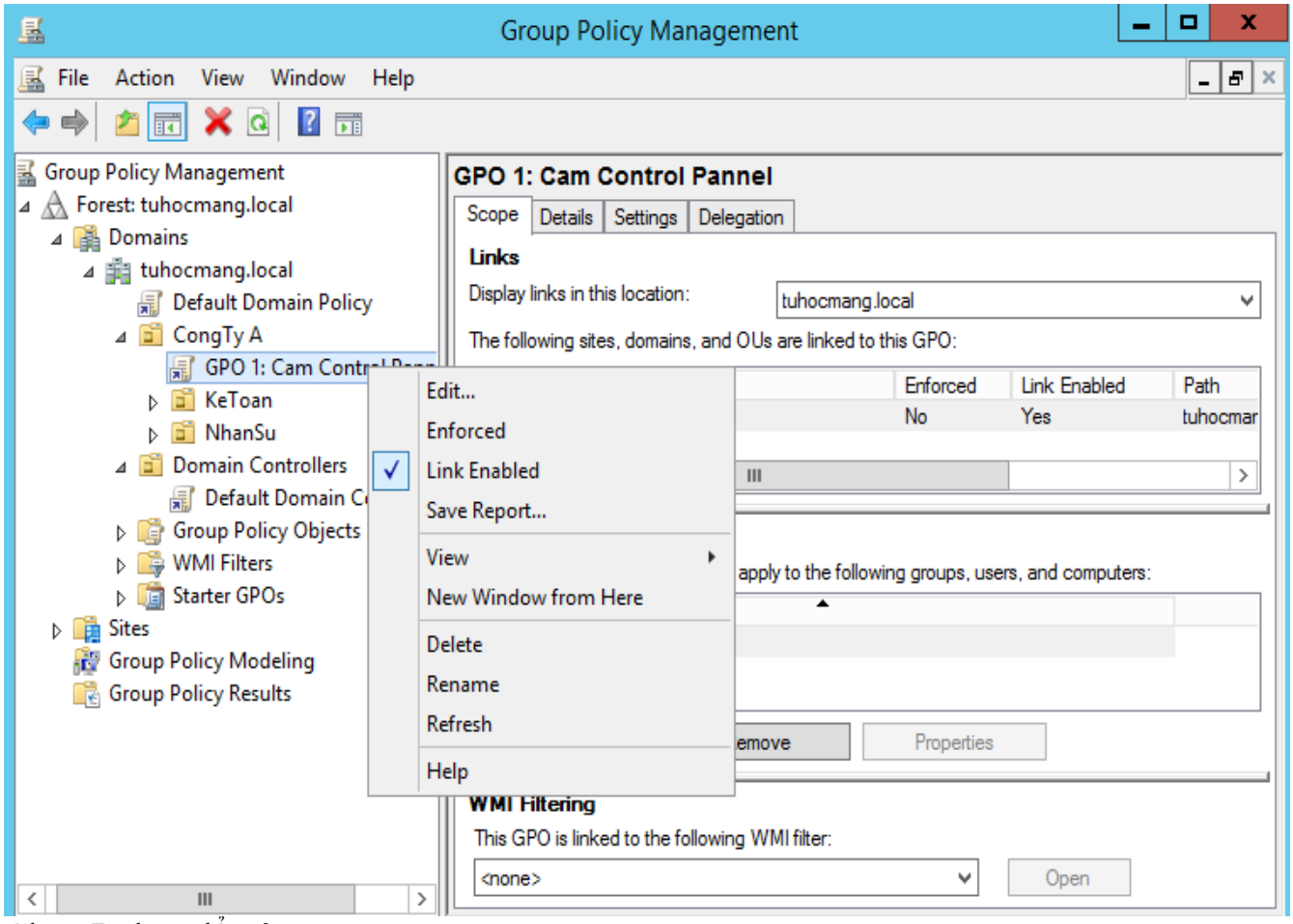


Select GPO

Tình huống:

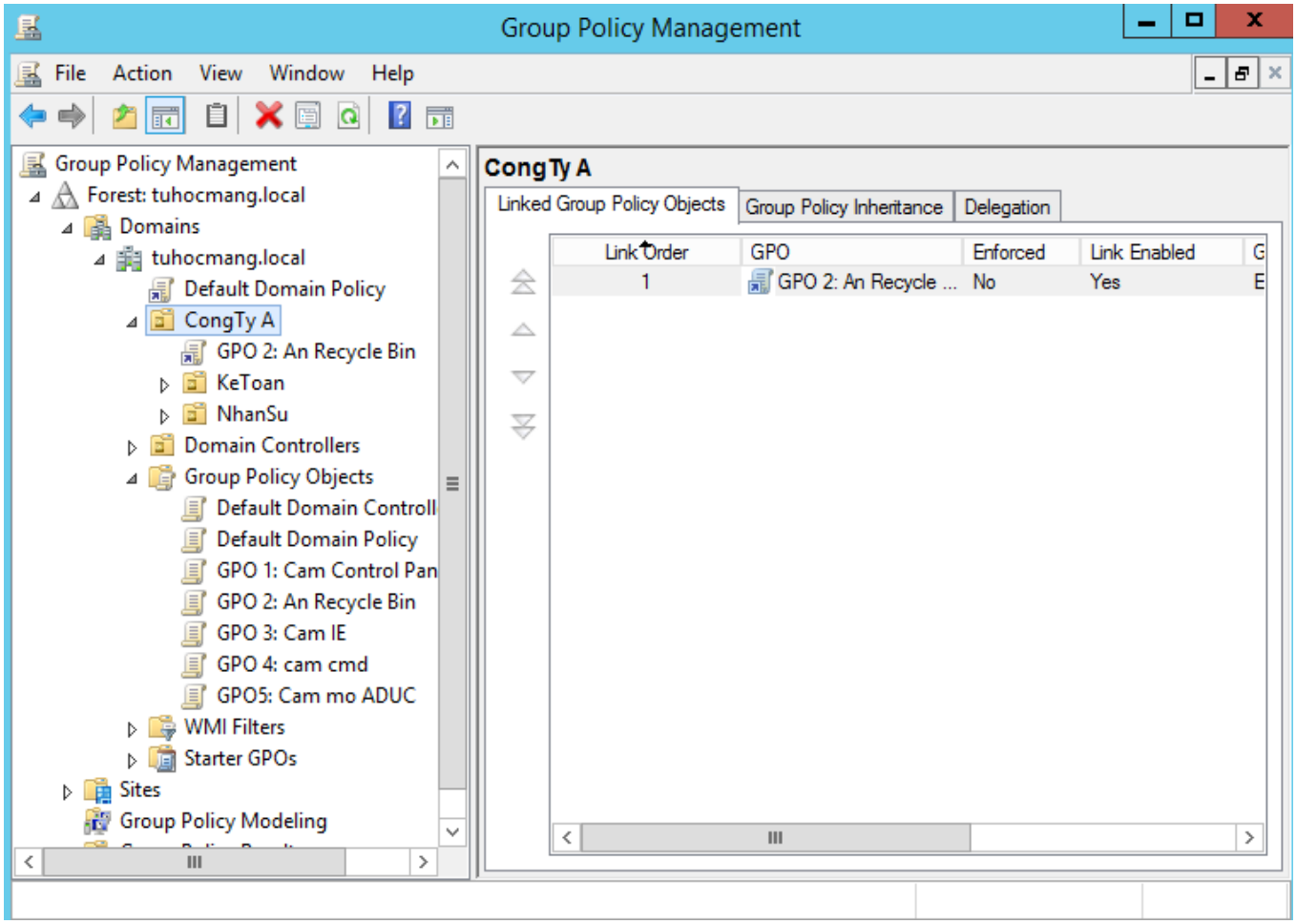
Khi thực hiện chính sách cấm Control Panel thì nhân viên than phiền nhiều nên ta muốn bỏ tác động của GPO 1 lên người dùng. Để bỏ tác động của GPO, ta có 2 cách:

Cách 1: xóa hẳn GPO (chỉ dùng khi tổ chức bỏ hẳn chính sách đó lên toàn công ty)



Chọn Delete để xóa

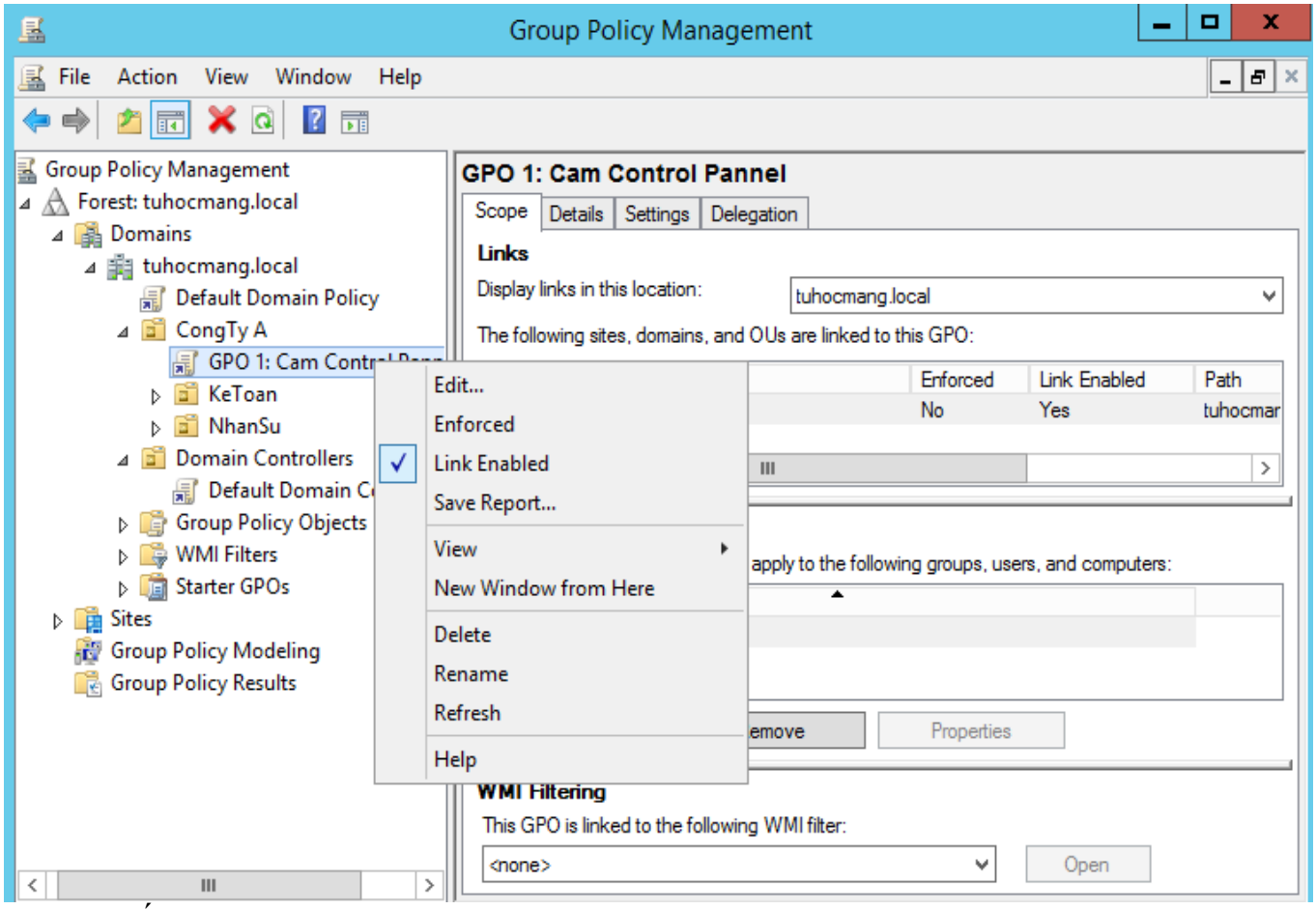
Chọn Delete.



Đã xóa GPO 1

Ta thấy sau khi bỏ thì OU CongTy mất GPO 1, nhưng GPO 1 vẫn còn tồn tại ở trong **Group Policies Object**. Nếu muốn dùng lại GPO 1 cho OU CongTy thì lại tiếp tục sử dụng tính năng "Link an existing GPO".

Cách 2: Bỏ tính năng Link GPO (Bỏ tính kế thừa của 1 GPO xuống các đối tượng con)



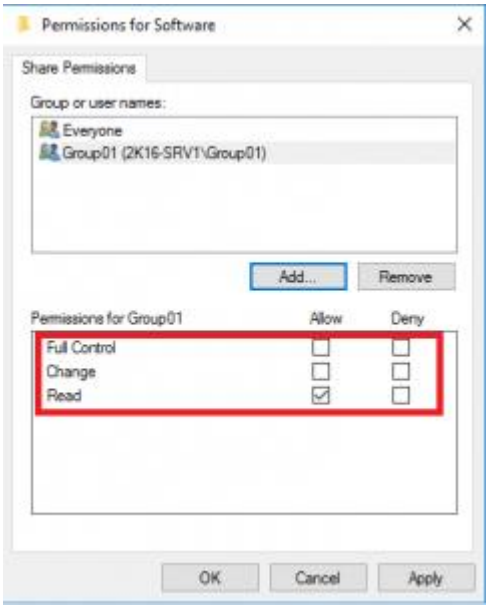
Bỏ tính kế thừa của GPO

Bỏ check Link Enabled

5. Chia sẻ dữ liệu và các quyền khi chia sẻ dữ liệu (share permission)

Chia sẽ dữ liệu (share) là một trong những công việc chủ yếu khi quản trị một mạng lớn hay nhỏ. Để tập trung quản lý dữ liệu thì người quản trị sẽ dùng một máy tính, máy tính đó có thể cài đặt Windows cho client như Windows 7, 8 hay 10 hoặc các Windows server…, chia sẻ các thư mục trên đó và cho phép người dùng truy cập, ghi chép… dữ liệu trên đó. Việc lưu trữ dữ liệu tập trung sẽ rất có ích trong việc backup dữ liệu, antivirus, tăng cường tính bảo mật.

Các quyền chia sẽ dữ liệu:



- **Read**: Cho phép user có thể xem và đọc (Read) các folder và file chứa trong thư mục share.
- **Change**: Cho phép user có thể xem/thực thi/ghi/xóa (read/execute/write/delete) folders/files.
- **Full control**: Cho phép users sử dụng tất cả các quyền của "Read," "Change," cũng như quyền chỉnh sửa và **lấy quyền sở hữu các tệp** (edit permissions and take ownership).

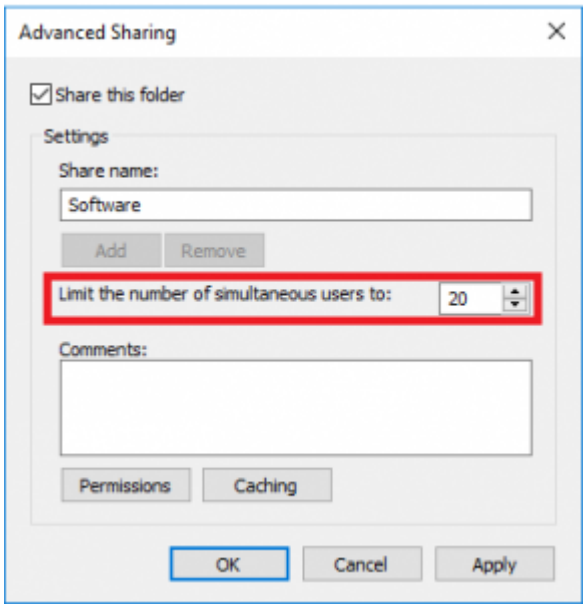
Các quyền NTFS được người quản trị cấu hình trên folder chia sẻ. Ví dụ: khi cho quyền **Share** là **Full control**, nhưng **NTFS** chỉ có quyền **Read**, thì user chỉ có thể **read** và không thể thực thi các quyền trong nhóm Change của Share Permission. Như vậy, để thực hiện được quyền share thì sẽ cần phân quyền NTFS tương ứng như sau:

		NTFS Basic Permission					
		Full control	Modify	Read&excute	List folder contents	Read	Write
Share Permission	Full control	x	x	x	x	x	x
	Change		x	x	x	x	x
	Read			x	x	x	

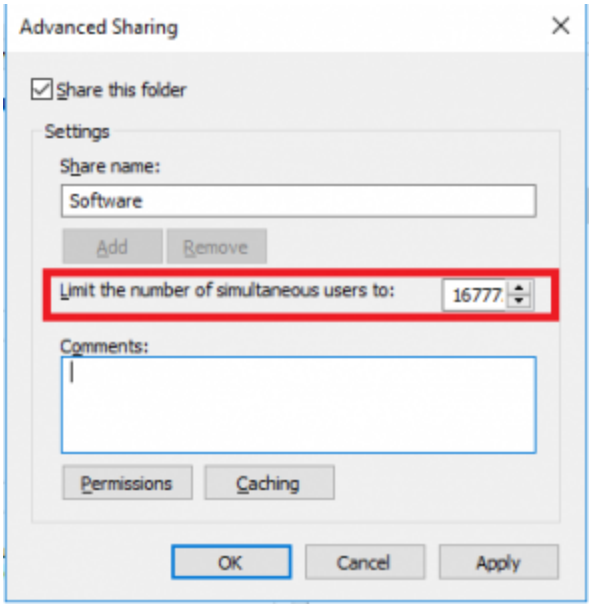
Lưu ý một khái niệm này, đó là **Share permission** là quyền truy cập dữ liệu từ xa qua mạng còn **NTFS** là quyền truy cập dữ liệu cụ thể trên một máy tính cụ thể. Nếu có quyền Share nhưng không có quyền NTFS thì sẽ không truy cập được dữ liệu và ngược lại. Điều đó có nghĩa là ***khi share một dữ liệu trên NTFS cho người dùng thì buộc ta phải cấp quyền NTFS tương ứng với quyền Share***.

Số lượng kết nối đồng thời vào thư mục share:

Số lượng kết nối đồng thời vào thư mục share phụ thuộc vào Windows đó là phiên bản Windows nào. Đối với các Windows client như Windows 7, Windows 8, Windows 10… thì số kết nối tối đa vào thư mục share là 20.

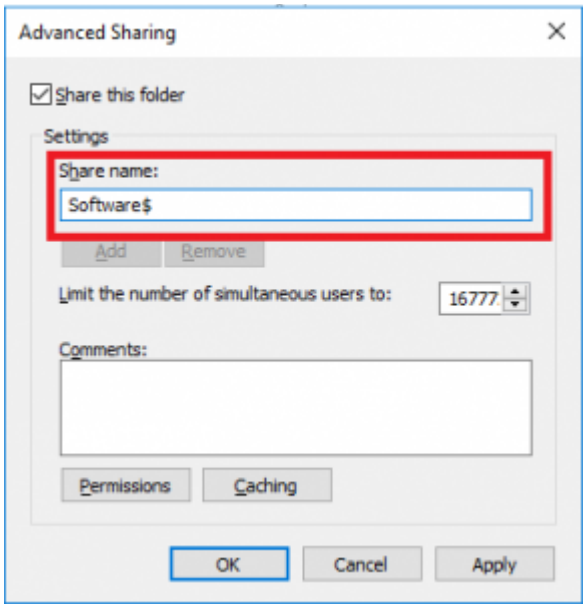


Đối với các Windows Server thì các kết nối đồng thời một thời điểm vào thư mục chia sẻ gần như không giới hạn với khoảng 16.777.216.



Share ẩn và share công khai:

Để share ẩn người ta thêm dấu $ phía sau cùng của Share name. Với share ẩn, user cần biết chính các tên của thư mục share là gì và điền chính xác tên đó cùng với dấu $ phía sau cùng thì mới có thể truy cập được.

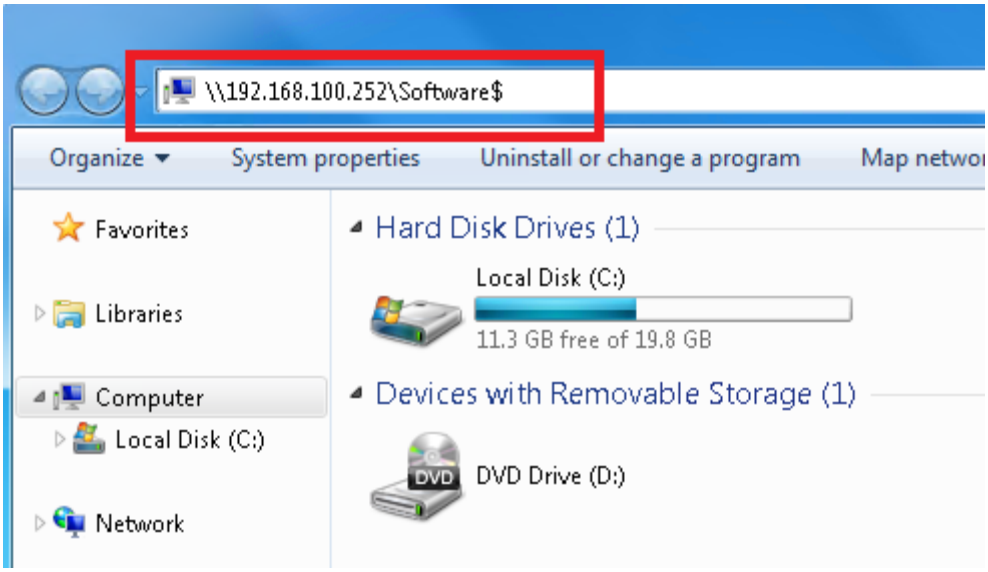


Đối với share công khai, người dùng không cần phải gõ chính xác địa chỉ và tên thư mục share, người dùng chỉ cần truy cập vào địa chỉ IP hoặc tên máy thực hiện share dữ liệu là được.

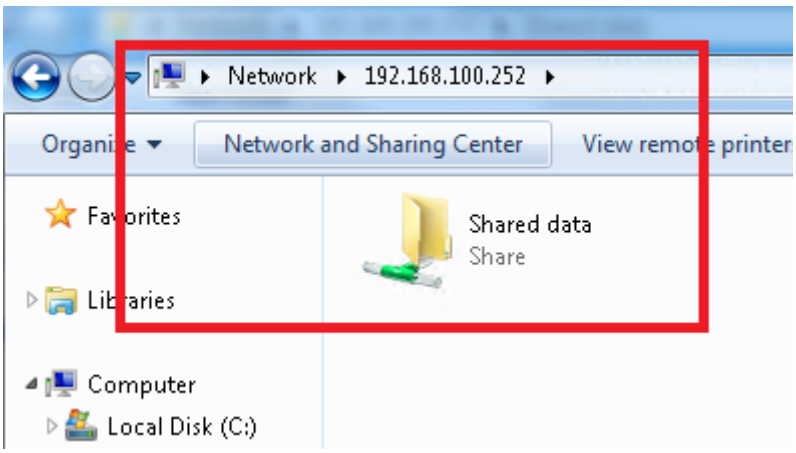
Truy cập dữ liệu share:

Để truy cập dữ liệu share, chúng ta dùng địa chỉ UNC (Universal Naming Convention) có dạng **\\{địa chỉ IP hoặc hostname}\{tên thư mục chia sẻ}**.

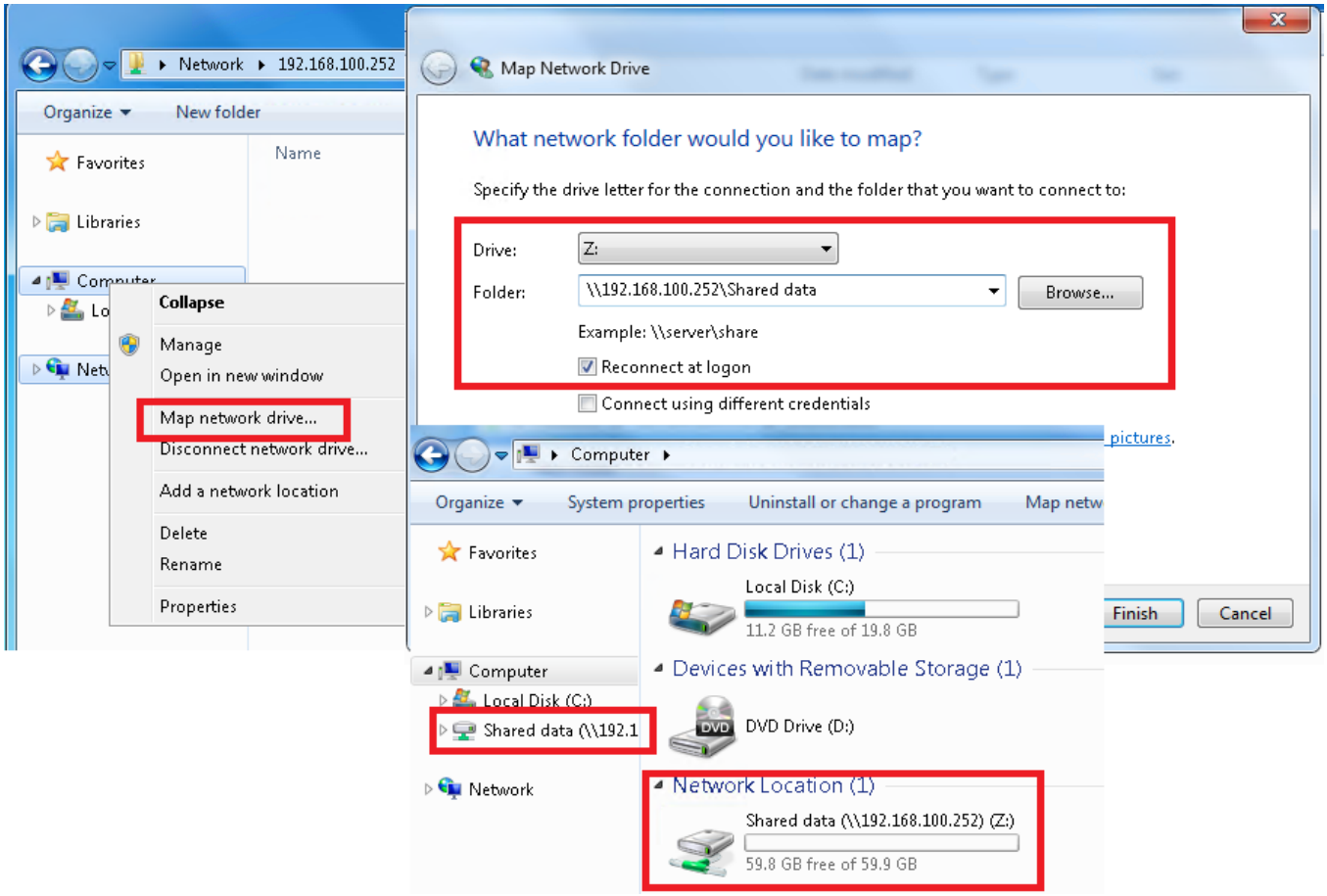
Đối với trường hợp share ẩn, cần phải gõ đầy đủ UNC là **\\{địa chỉ IP hoặc hostname}\{tên thư mục chia sẻ}$**



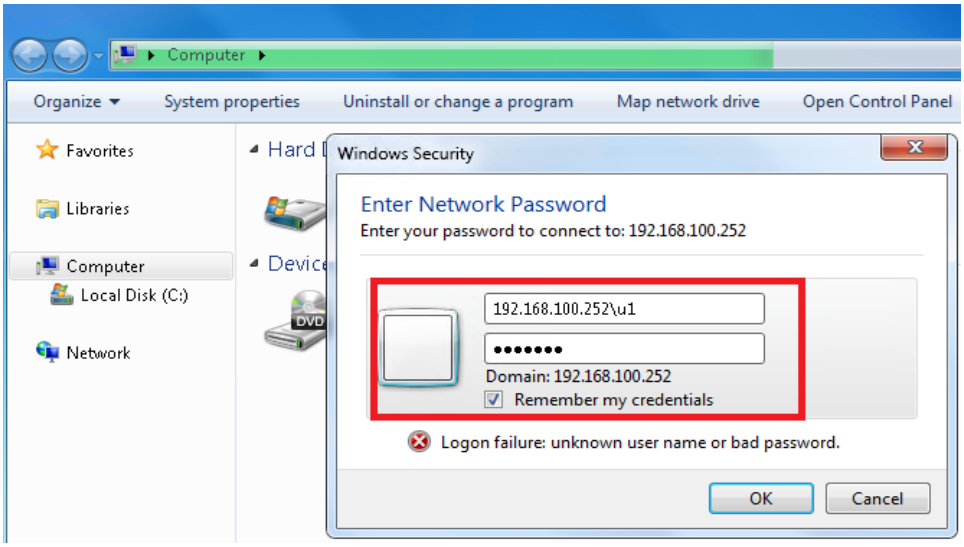
Đối với trường hợp không share ẩn thì chỉ cần gõ **{địa chỉ IP hoặc hostname}** trên thanh address của Windows Explorer, sau đó các thư mục chia sẻ sẽ được liệt kê và bạn có thể truy cập vào thư mục mình mong muốn.



Đối với trường hợp các thư mục chia sẻ mà ta thường xuyên sử dụng, có thể map chúng về thành một ổ đĩa mạng và khi truy cập, ta không cần phải gõ UNC nữa.



Khi truy cập dữ liệu chia sẻ, ta phải nhập username và password được cấp trên máy chia sẻ thư mục ({**IP hoặc tên may chia sẻ}\{username}**). Đối với trường hợp hệ thống Doamin Controller, với các máy tính cùng join vào một domain thì chúng không cần bước xác thực này.



Nếu ta không muốn chứng thực thì có thể sử dụng phương thức share không cần chứng thực, nhưng như vậy hoàn toàn không an toàn cho dữ liệu bởi vì bất cứ ai có thể kết nối với mạng của ta đều có thể thấy được dữ liệu chia sẽ trong mạng đó.

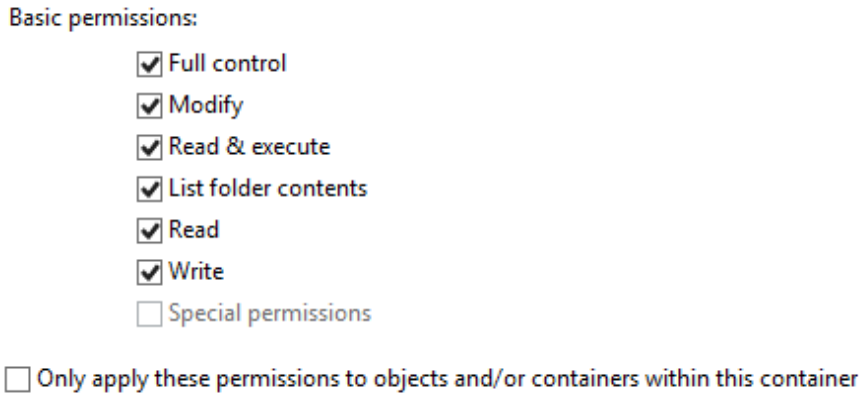
6. Quyền truy cập NTFS (NTFS Permissions) – Access Control List-ACL

NTFS: ***New Technology File System*** là hệ thống tập tin tiêu chuẩn của Windows NT, bao gồm cả các phiên bản Windows 2000 trở về sau này. NTFS thay thế hệ thống tập tin FAT dành cho các hệ điều hành Windows của Microsoft. NTFS có nhiều cải tiến hơn FAT như hỗ trợ cải tiến cho các siêu dữ liệu và sử dụng các cấu trúc dữ liệu tiên tiến để cải thiện hiệu suất, độ tin cậy, sử dụng không gian ổ đĩa, cộng thêm phần mở rộng như các danh sách kiểm soát truy cập bảo mật (Access Control List-ACL) và bản ghi hệ thống tập tin. Số lượng tập tin tối đa trong 1 phân vùng 4.294.967.295 ($2^{32} - 1$), hỗ trợ tối đa dung lượng ổ đĩa là 16 EiB (Exbibyte, 1 EiB = 1.073.741.824 gigabytes) trên thực tế là 256 TiB (tebibyte, 1 TiB = 1,024 gibibytes).

Ta đề cập đến danh sách kiểm soát truy cập bảo mật (Access Control List-ACL) hay được gọi với một cái tên khác là NTFS Permissions và tiếng Việt hay gọi là phân quyền NTFS.

NTFS Permissions là hệ thống tập hợp các quyền cho phép hoặc không cho phép nhóm người dùng (Group) hay người dùng (User) truy cập vào các đối tượng chứa trên một phân vùng NTFS bao gồm các thư mực (folder) và tập tin (file).

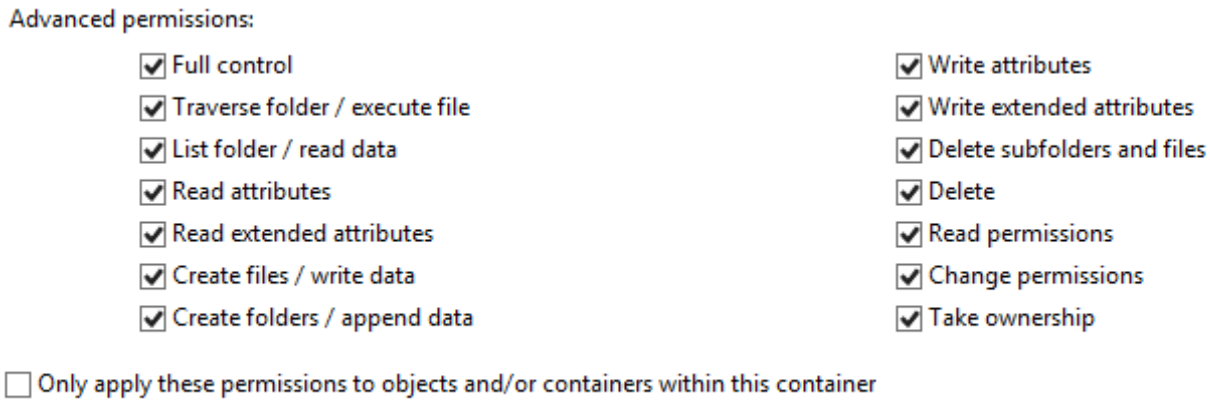
Các quyền cơ bản trên hệ thống NTFS bao gồm (Basic permissions):



Permission	Tác dụng trên Folder	Tác dụng trên File
Full control	Người dùng có toàn quyền kiểm soát vào thư mục và có thể thêm, thay đổi, di chuyển và xóa các mục. Người dùng cũng có thể thêm và loại bỏ quyền truy cập vào thư mục, cũng như đối với bất kỳ thư mục con.	Người dùng có toàn quyền kiểm soát các tập tin và có thể thay đổi, di chuyển hoặc xóa nó. Người dùng cũng có thể thêm và loại bỏ quyền truy cập vào các tập tin
Modify	Một sự kết hợp của Write và Read. Người dùng cũng có khả năng để xóa các tập tin trong một thư mục được cấp quyền Modify. Người dùng cũng có thể xem nội dung của thư mục con.	Người dùng có thể sửa đổi các nội dung của các tập tin được cấp quyến này.
Read & execute	Người dùng được phép đọc các nội dung của các tập tin trong thư mục hoặc thực hiện các chương trình bên trong thư mục.	Người dùng được phép đọc các nội dung của tập tin hoặc thực hiện thực thi các chương trình.
List folder contents	Cho phép người dùng xem nội dung của thư mục đã chọn. Người dùng không được phép đọc nội dung của một tập tin hoặc thực hiện một tập tin.	Quyền này không áp dụng cho mức độ tập tin
Read	Người dùng có thể đọc nội dung của một thư mục.	Người dùng có thể đọc nội dung của một tập tin.
Write	Người dùng có thể tạo ra các tập tin và thư mục. Này không cấp cho người dùng với khả năng đọc những thông tin hiện có.	Người dùng có thể tạo ra một tập tin và ghi thêm dữ liệu vào tập tin.

Như vậy, ta có thể thấy rằng việc cấp quyền Full control thì ngời dùng sẽ có quyền rất cao, việc này sẽ ảnh hưởng đến bảo mật của hệ thống, vì vậy quyền này nên hạn chế sử dụng.

Ở trong các quyền cơ bản trên, có một quyền là **Special Permissions**, quyền này là quyền đặc biệt, nó chỉ được check khi bạn tiến hành cấu hình thêm các quyền nhỏ trong **Advanced permissions**. Với **Advanced permissions** sẽ giúp người quản trị có thể phân quyền chi tiết hơn :



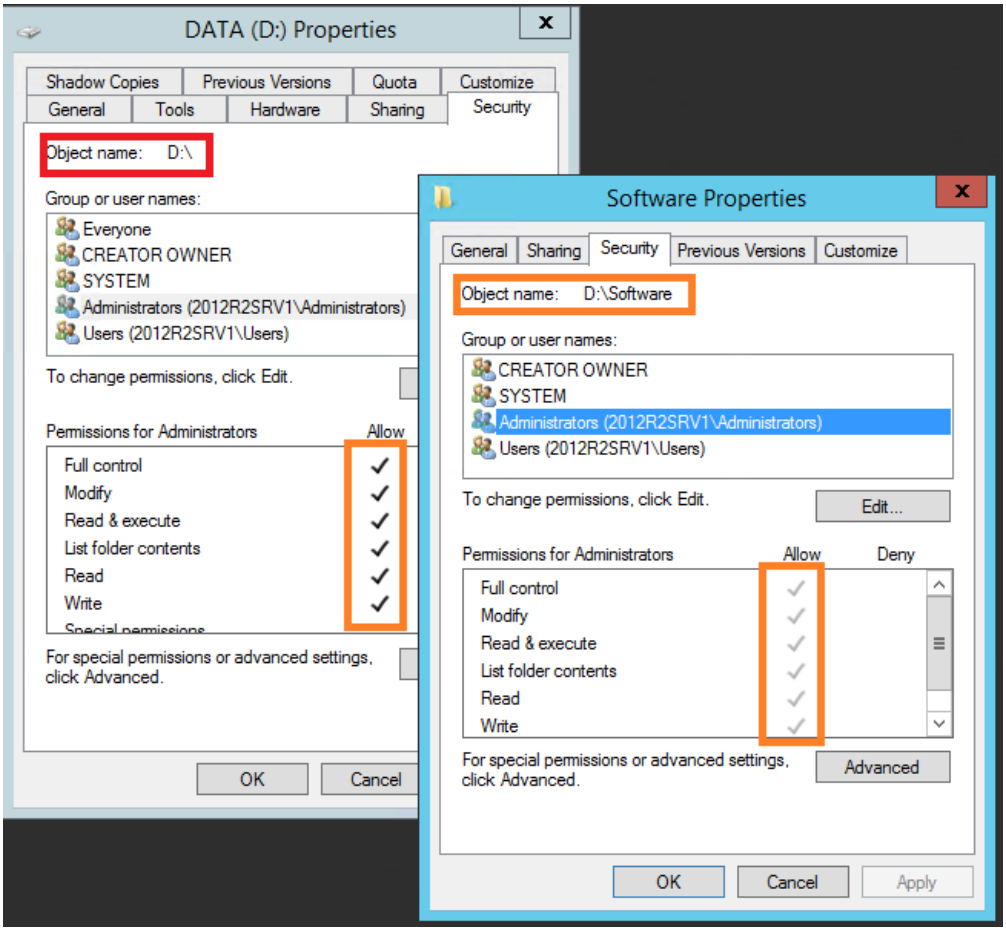
Special permissions	Full Control	Modify	Read & Execute	List Folder Contents (folders only)	Read	Write
Traverse Folder/Execute File	x	x	x	x		
List Folder/Read Data	x	x	x	x	x	
Read Attributes	x	x	x	x	x	
Read Extended Attributes	x	x	x	x	x	
Create Files/Write Data	x	x				x
Create Folders/Append Data	x	x				x
Write Attributes	x	x				x
Write Extended Attributes	x	x				x
Delete Subfolders and Files	x					
Delete	x	x				
Read Permissions	x	x	x	x	x	x
Change Permissions	x					
Take Ownership	x					
Synchronize	x	x	x	x	x	x

Trong **Advanced permissions** có một quyền đặt biệt, quyền **Take ownership**, quyền này cung cấp cho người quản trị (administrator) chiếm quyền trên phân vùng, thư mục hoặc tập tin. Ví dụ như trong trường hợp máy tính của bạn phải cài lại Windows, nhưng trong quá trình sử dụng của hệ điều hành cũ, qua hệ điều hành mới các user này không còn tồn tại do khác SID dẫn đến tình trạng mất quyền truy cập vào tài nguyên, lúc đó người quản trị có thể dùng quyền **Take ownership** để chiếm quyền là phân lại quyền truy cập.

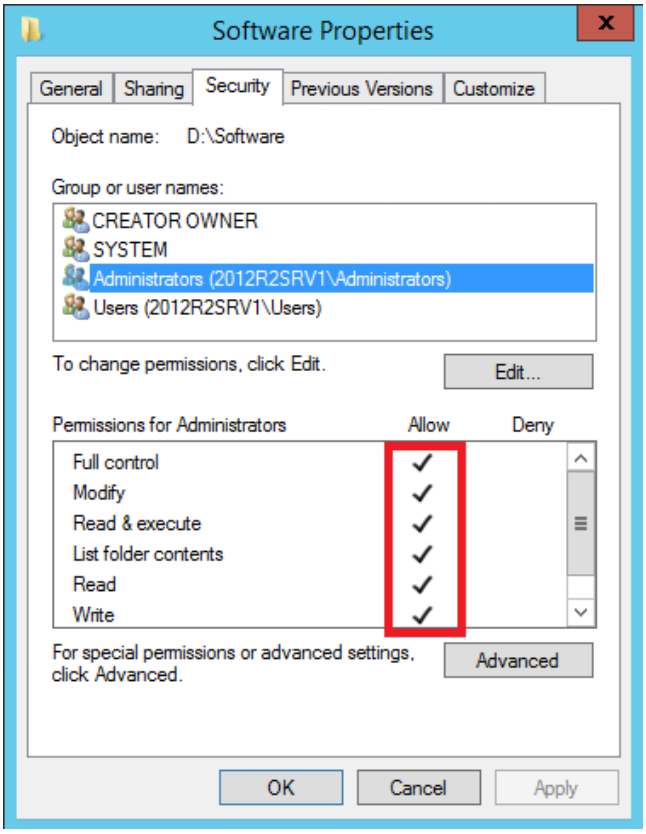
Tính kế thừa (inheritance) NTFS Permission:

Mặc định NTFS sẽ có tính kế thừa như sau:

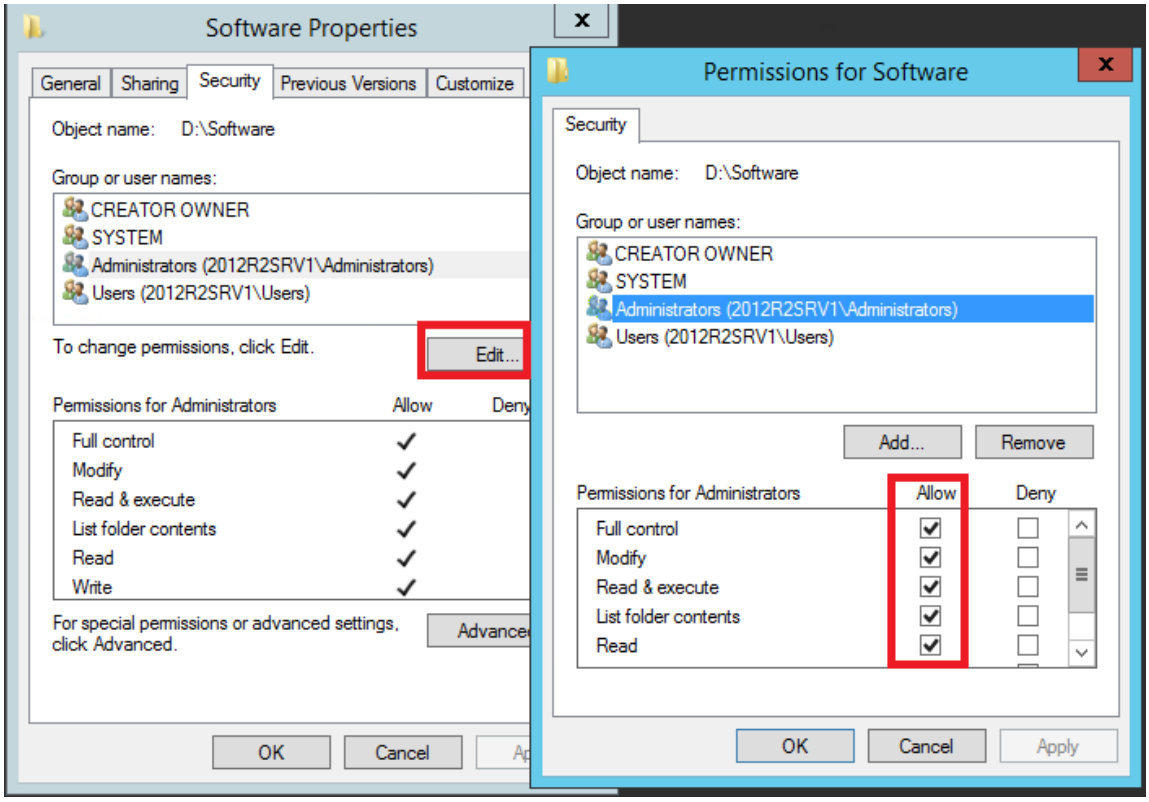
- Các file và folder được tạo trên một phân vùng định dạng NTFS thì nó sẽ kế thừa các quyền từ phân vùng.
- Các file và folder sẽ thừa kế quyền từ các folder cha chứa chúng.



Các quyền NTFS kế thừa sẽ có dấu check bị mờ đi, chúng ta có thể thấy khi xem thuộc tính (Properties) của thư mục **Software** là thư mục nằm trong phân vùng ổ đĩa **D**. Để có thể phân quyền lại, ta phải loại bỏ tính kế thừa (**inheritance**) của thư mục cần phân quyền.



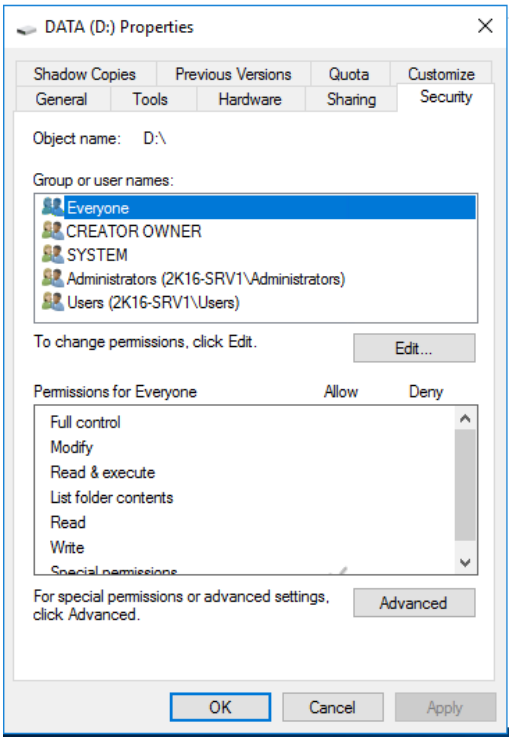
Sau khi bỏ kế thừa quyền, chúng ta có thể phân quyền lại.



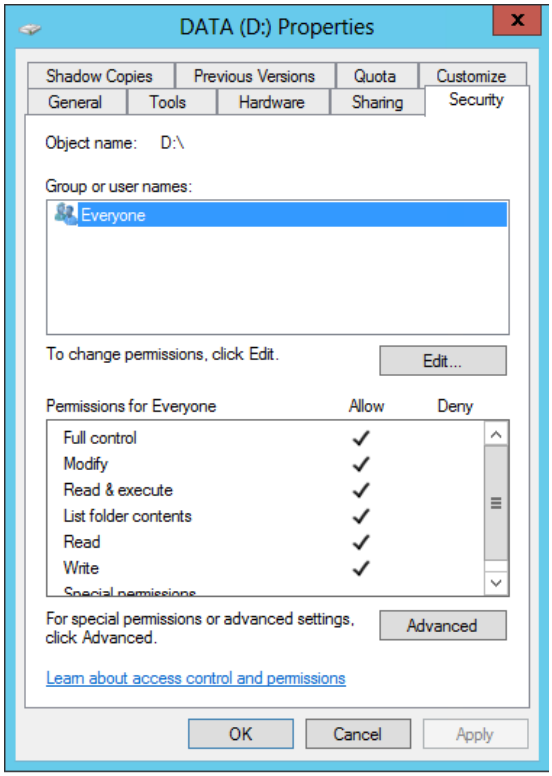
7. Phân quyền NTFS (NTFS Permissions)

Ở phần trên đã đề cập các quyền NTFS, bao gồm quyền Basic permissions và Advanced permissions, trong phần này sẽ đề cập chi tiết đến việc cấp quyền cho người dùng và các nhóm người dùng. Như đã biết, khi thư mục được tạo trên phân vùng NTFS nó sẽ thừa kế các quyền có sẵn trên phân vùng.

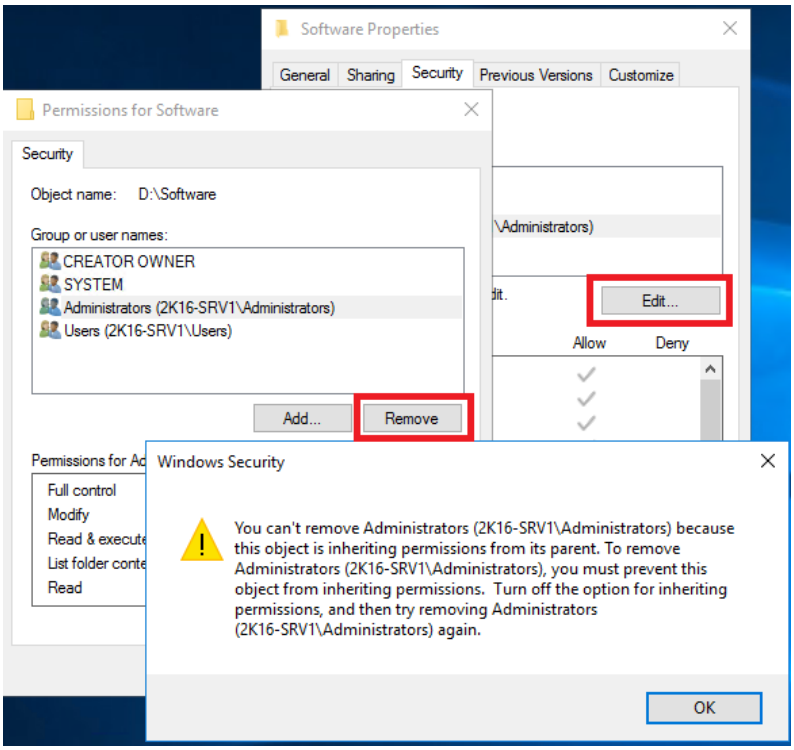
Khi định dạng bằng Windows.



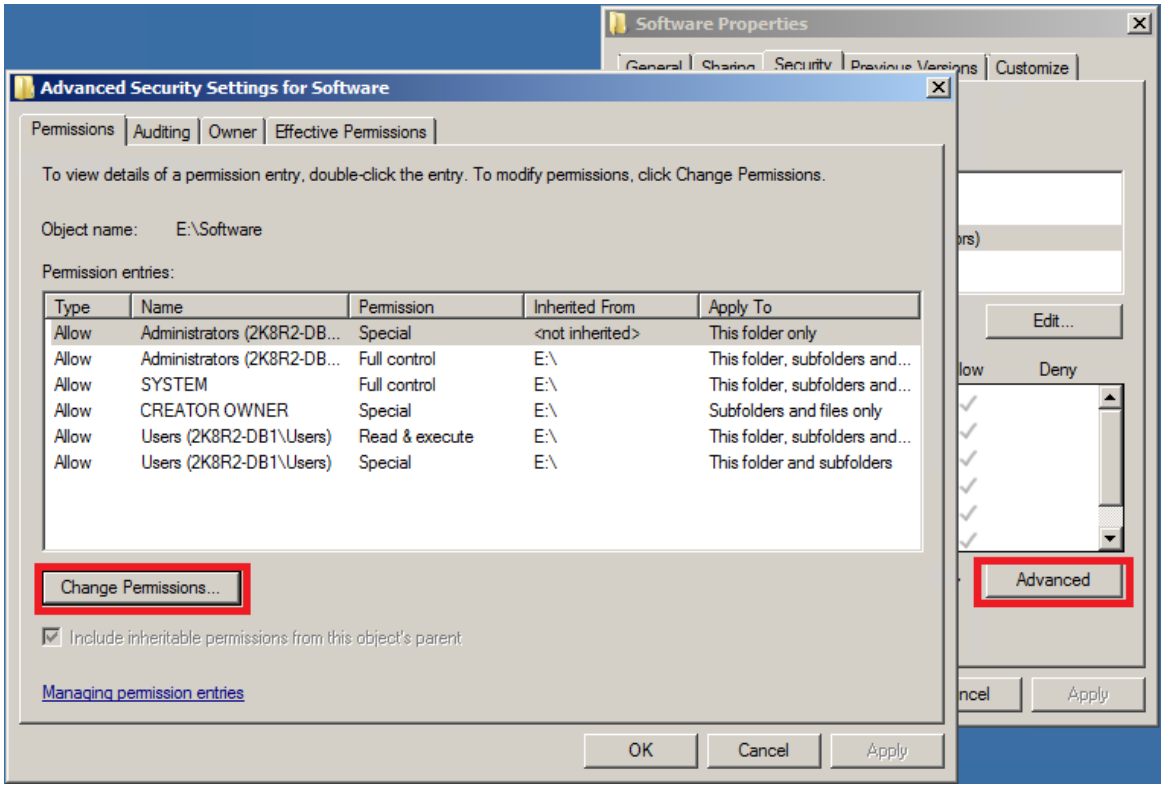
Khi định dạng bằng phần mềm khác như Acronis trong Hiren's boot.



Do thừa kế quyền từ phân vùng NTFS, chúng ta cũng không thể remove các user đang có quyền trên đó, cũng không thể thay đổi quyền của các user có sẵn.

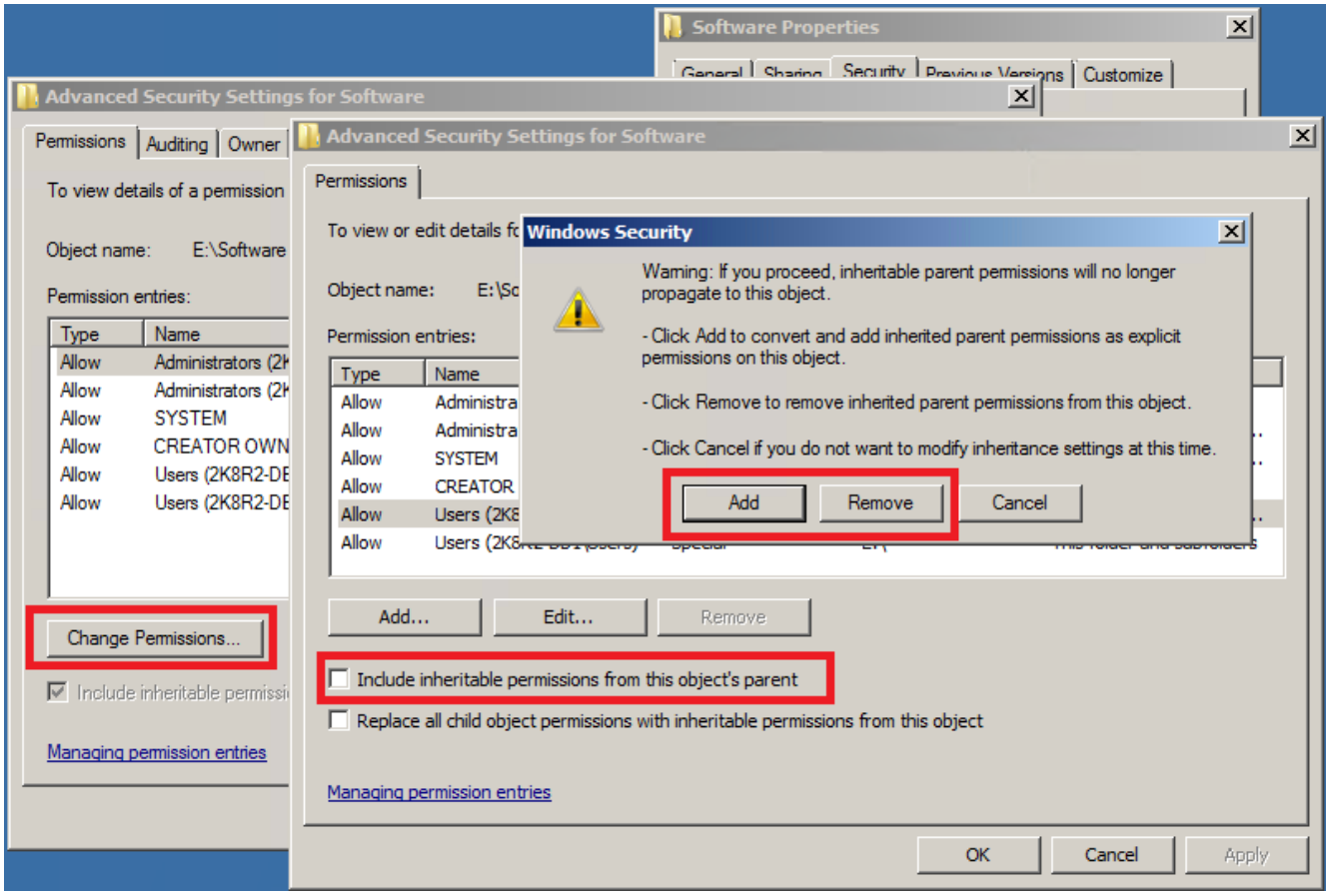


Để có thể phân quyền NTFS lại hoặc loại bỏ các quyền được kế thừa, trong hộp thoại **Properties**, chọn tab **Security**, chọn nút **Advanced, chọn Change Permissions…**

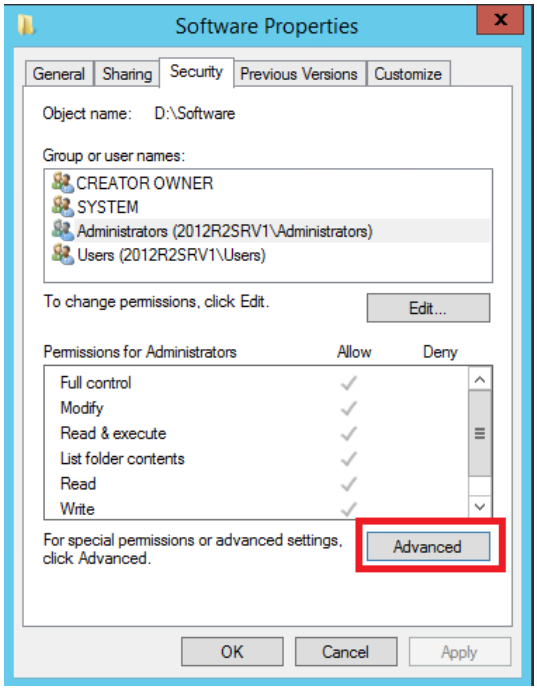


Với ***Windows 7,*** trong hộp hoại tiếp theo, bạn chọn bỏ dấu check ở dòng **Include inheritable permissions from this object's parent.** Tiếp theo, hộp thoại **Windows Security** bật lên, có hai tùy chọn:

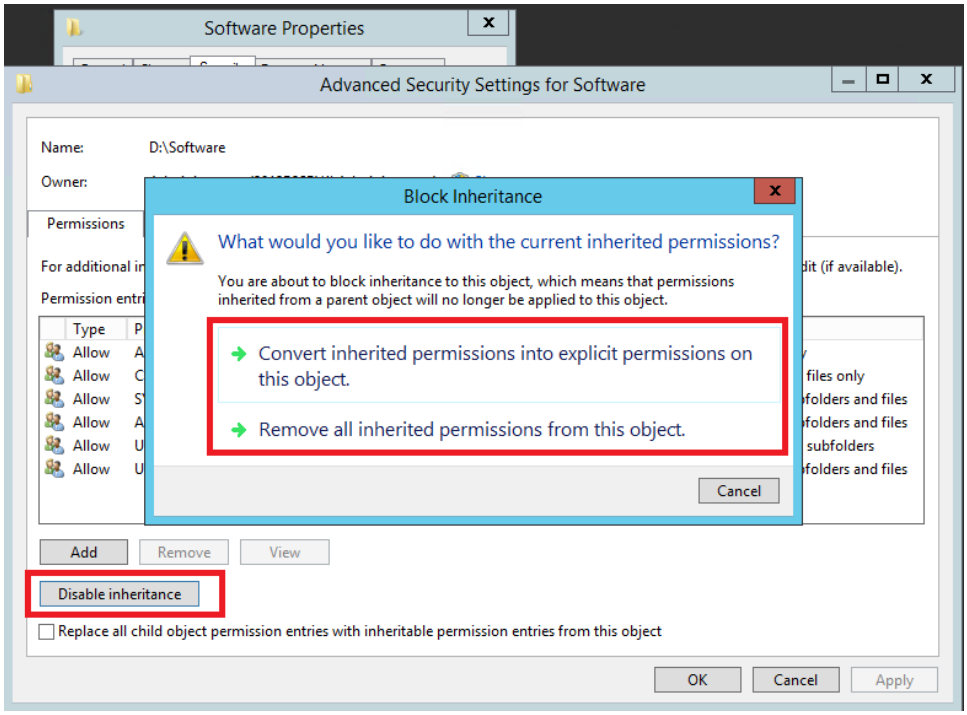
- **Add**: cho phép giữ lại các quyền hiện tại, người quản trị chỉ cần cấu hình lại.
- **Remove**: Loại toàn bộ quyền và các tài khoản đang có.



Trên Windows 8, Windows 10, Windows 2012, Windows Server 2016: Trong hợp thoại **Properties**, chọn tab **Security**, chọn nút **Advanced**



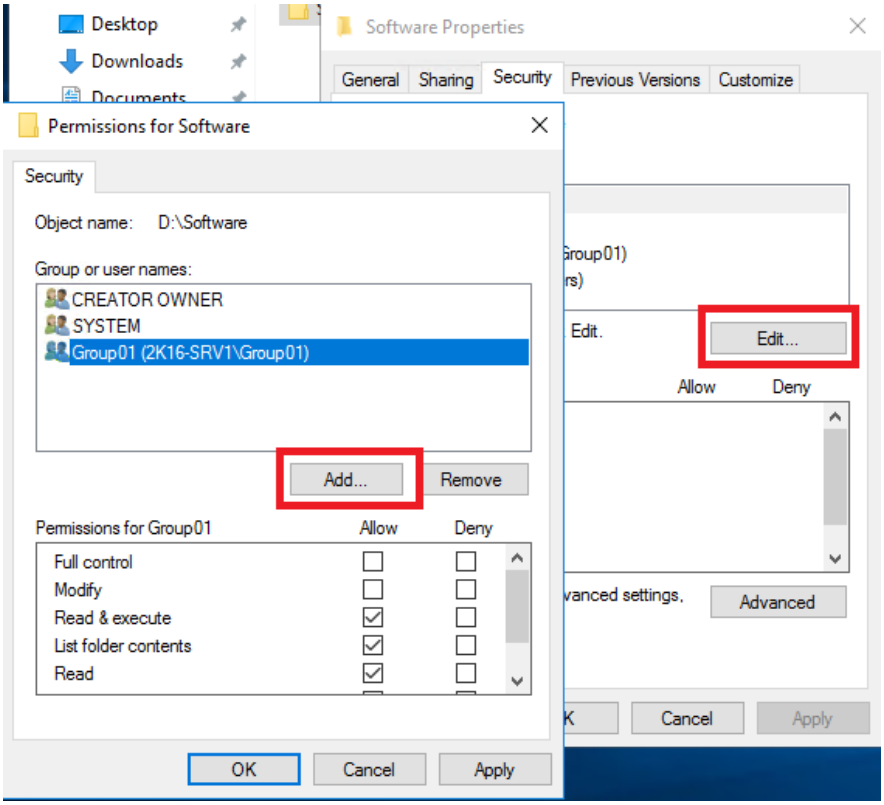
Trong hộp thoại **Advanced Security Setting…**, chọn **Disable inheritance**.



Trong hộp thoại **Block Inheritance** có hai hộp thoại:

- **Covert inherited permissions into explicit permissions on this object**: giữ lại các quyền hiện có và cấu hình lại.
- **Remove all inherrited permissions from this object**: loại bỏ các quyền hiện có và cấu hình lại.

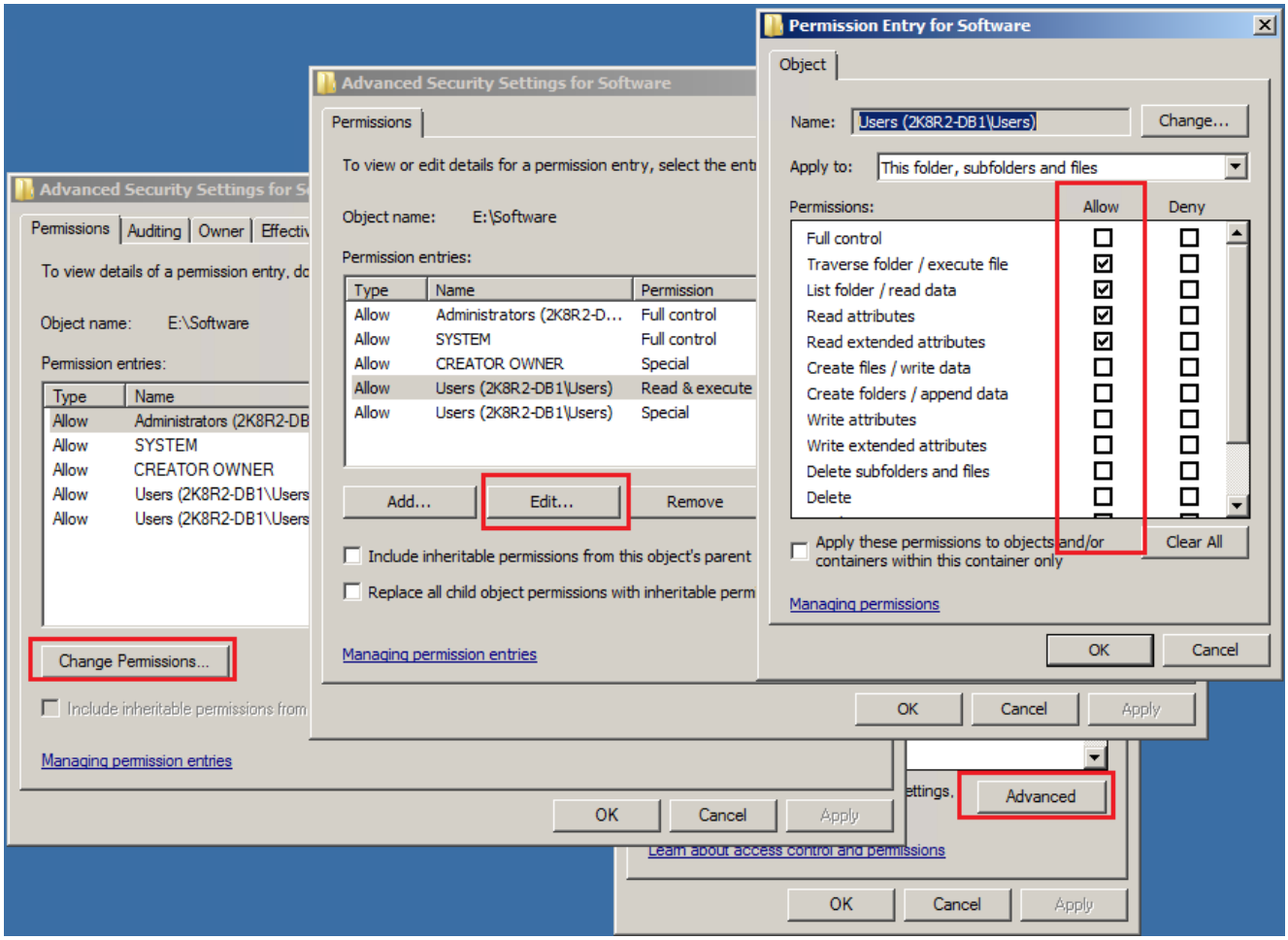
Basic Permissions: Sau khi loại bỏ các quyền kế thừa, Add hoặc remove các user và group, cũng như tiến hành phân quyền lại cho người dùng có sẵn.



***Advanced Permissions* (tham khảo bảng các quyền trong phần *NTFS Permissions*):** *có thể thay đổi các quyền chi tiết hơn.*

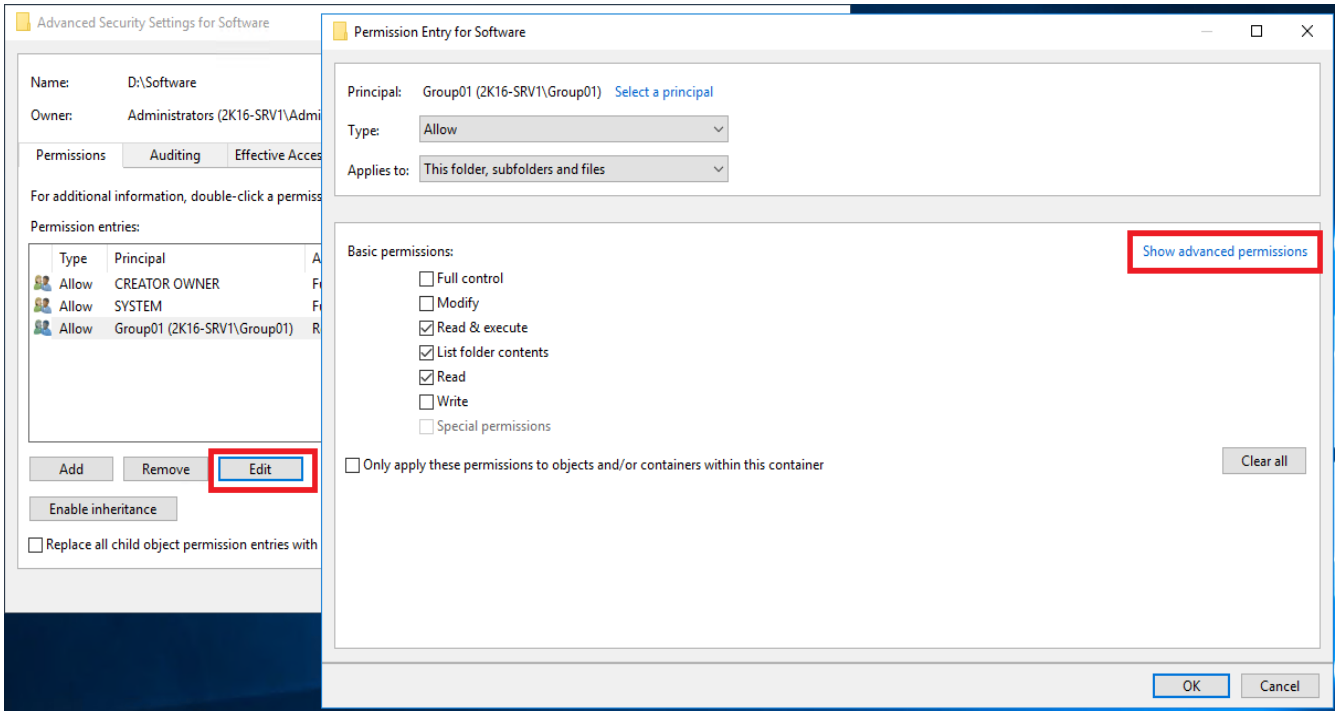
Trên Windows 7, Windows Server 2008:

Trong hộp thoại **Properties**, tab **Security**, chọn **Advanced**, trong hộp thoại tiếp theo chọn **Change Permissions…**, tiếp theo chọn lên user hoặc group cần phân quyền, chọn **Edit**.

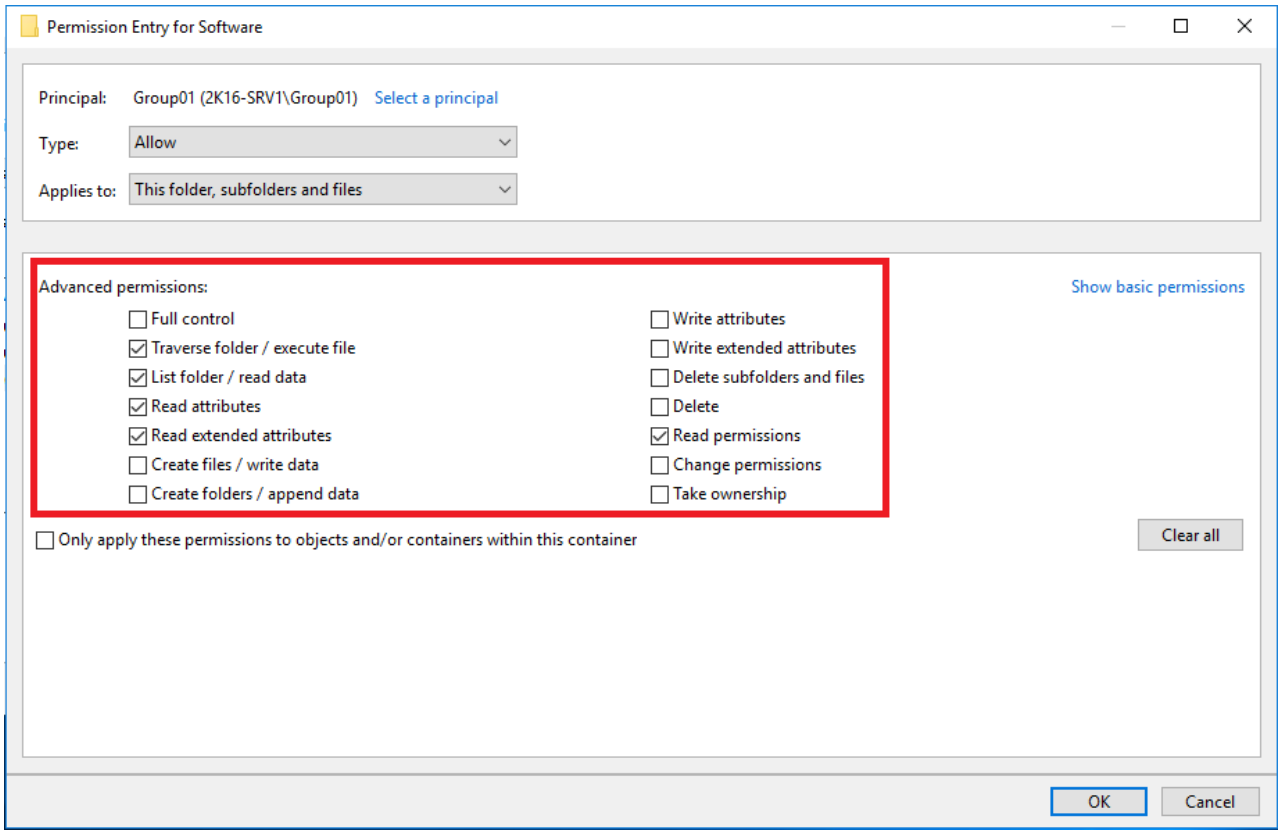


Trên Windows 8,Windows 10, Windows 2012, Windows Server 2016:

Trong hộp thoại **Properties**, tab **Security**, chọn **Advanced**. Chọn user cần phân quyền, chọn **Edit**. Trong hộp thoại **Permission Entry**, chọn **Show advanced permission**.



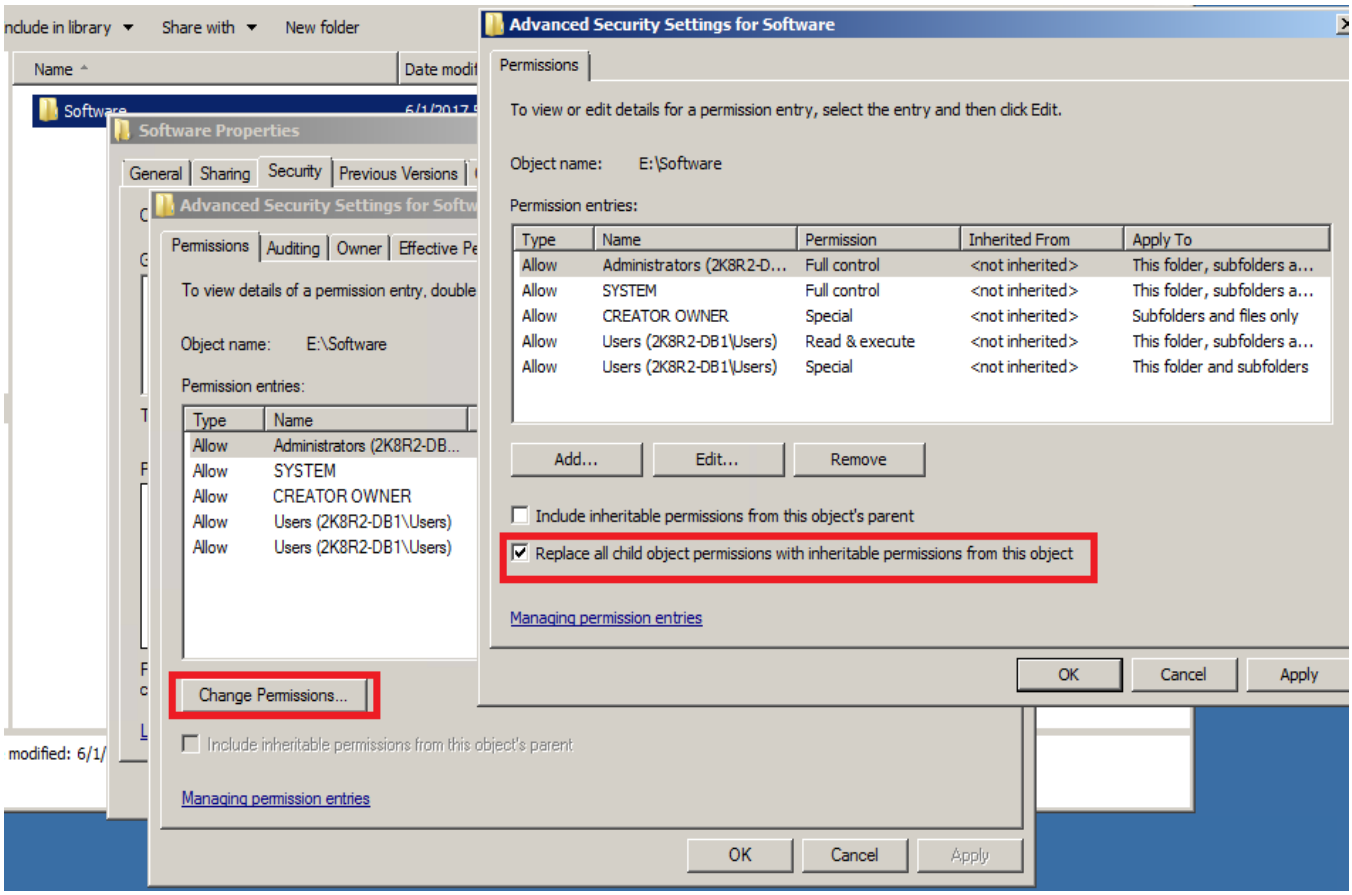
Tiếp theo thay đổi các quyền.



Sau khi phân quyền mới xong, nếu muốn các quyền này sẽ được áp dụng cho các thư mục và tập tin bên trong của nó, có thể Replace các quyền xuống cho các thư mục con:

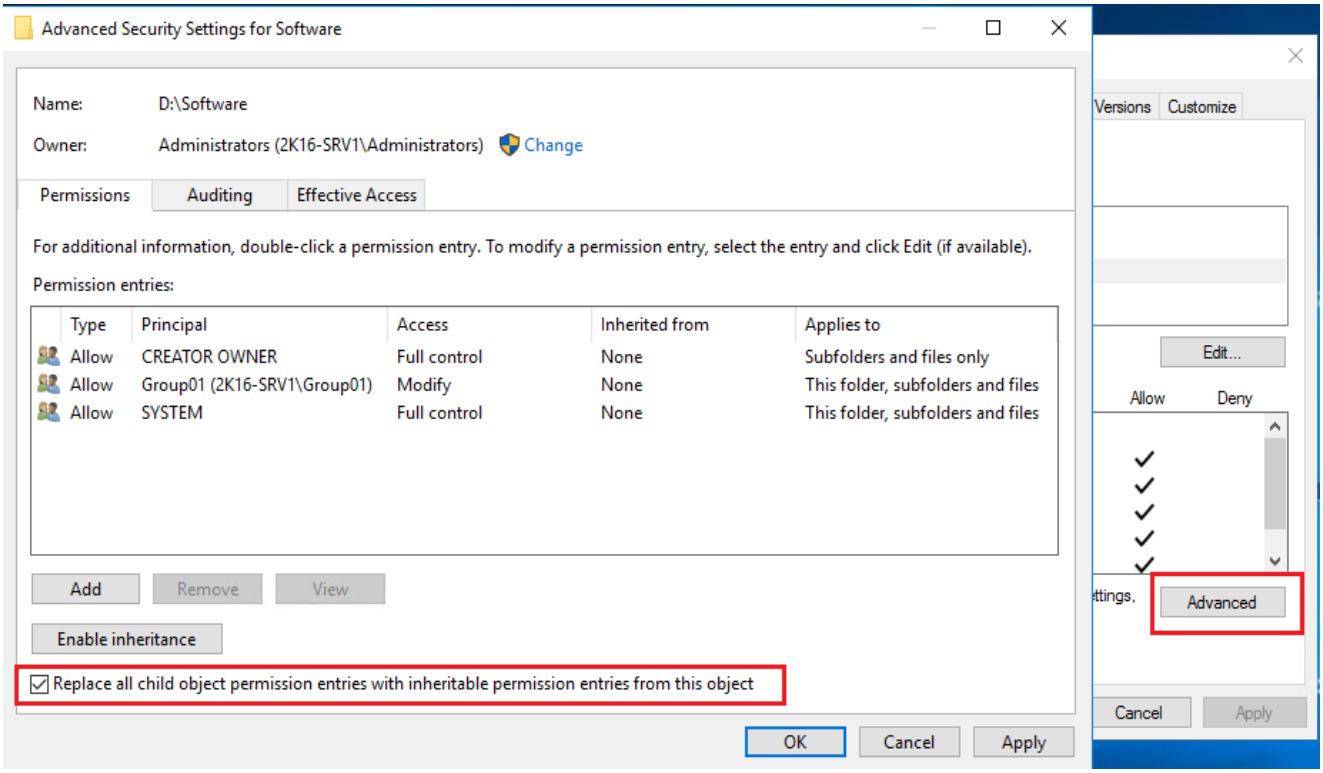
Trên Windows 7, Windows Server 2008:

Trong hộp thoại **Properties**, chọn tab **Security**, chọn nút **Advanced, chọn Change Permissions…** Trong hộp thoại tiếp theo, chọn check lên dòng **Replace all child object permission with inheritable permissions from this object**. Sau khi, Apply và OK tất cả các hộp thoại thì quyền của folder cha sau khi được phân quyền NTFS lại sẽ được áp dụng cho các folder con và file nằm trong folder cha.



Trên Windows 8,Windows 10, Windows 2012, Windows Server 2016:

Trong hộp thoại **Advanced Security Setting…**, chọn check lên dòng **Replace all child object permission with inheritable permissions from this object**. Sau khi, Apply và OK tất cả các hợp thoại thì quyền của folder cha sau khi được phân quyền NTFS lại sẽ được áp dụng cho các folder con và file nằm trong folder cha.



Lưu ý là bạn chỉ chọn được **Replace all child object permission with inheritable permissions from this object** khi folder có chứa folder con hoặc file, nếu folder không có chứa gì bên trong nó thì chọn **Replace all child object permission with inheritable permissions from this object** hệ thống sẽ báo lỗi.